

Titlul original: **Wireless Networks first-step**

Authorized translation from the English language edition, entitled WIRELESS NETWORKS FIRST-STEP, 1st Edition, 1587201119, by Jim Geier, published by Pearson Education, Inc, publishing as Cisco Press, Copyright © 2005 by Cisco Systems, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc. Romanian language edition published by Editura CORINT, Copyright © 2005.

Copyright © 2005 CORINT

Toate drepturile asupra versiunii în limba română aparțin Editurii CORINT, parte componentă a Grupului Editorial Corint.

Nici o parte din această carte nu poate fi reprodusă ori transmisă în orice formă sau prin orice mijloace, electronice sau mecanice, inclusiv fotocopiare, înregistrare sau prin orice sistem de stocare a informației fără acordul prealabil scris al Editurii CORINT.

Coordonare colecție IT: **Alice Raluca PETRESCU**
Tehnoredactare computerizată: **Alexandru MITREA**
Copertă: **Alexandru MITREA**

Difuzare:

Str. Teodosie Rudeanu nr. 21, sectorul 1, București
Tel.: (021) 222.19.49; 222.40.34; 223.19.28. Fax: (021) 222.71.78.
www.edituracorint.ro;
e-mail: vanzari@edituracorint.ro

Descrierea CIP a Bibliotecii Naționale a României
GEIER, JIM

Primii pași în rețele fără fir/ Jim Geier; trad.:
Cristian Mihai, București - Corint, 2005

Index

ISBN 973-653-709-9

I. Mihai Cristian (trad.)

654

Tipărit la S.C. DON-STAR S.R.L. Galați, Str. 1 Decembrie 23
Tel./Fax: 0236-492587

Jim Geier

Primii pași în **REȚELE FĂRĂ FIR**

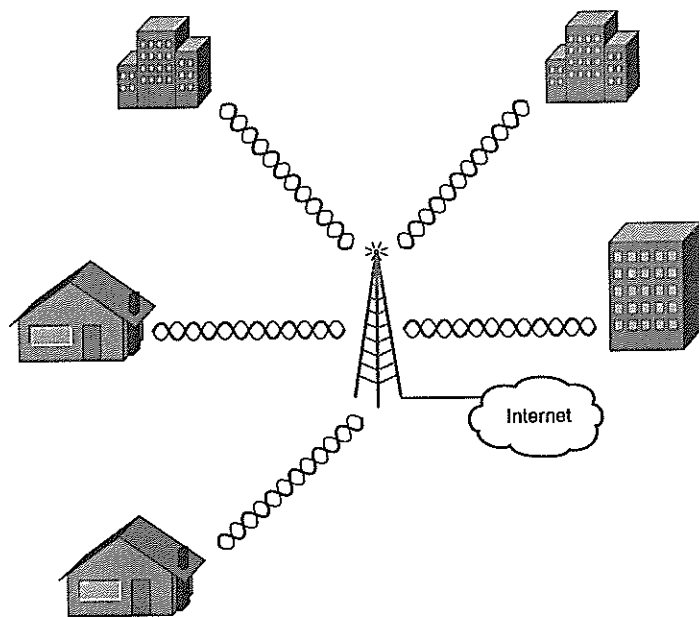
Traducerea: Cristian MIHAI

CORINT
București, 2005

furnizoare de energie electrică poate instala o rețea MAN fără fir printr-un oraș pentru a asigura accesul la comenzi de lucru din diferite locații. Prin urmare, MAN-urile fără fir pot conecta infrastructuri de rețele existente pentru a permite utilizatorilor mobili să comunice cu acestea.

Furnizorii de servicii Internet fără fir (în limba engleză: Wireless Internet Service Providers — acronim WISP) instalează MAN-uri fără fir în marile orașe și în zonele rurale pentru a asigura conexiuni fără fir fixe, pentru locuințe și firme, așa cum se arată în figura 1.3. O rețea MAN fără fir oferă avantaje importante în situațiile în care instalarea conexiunilor tradiționale prin fir (cum ar fi Digital Subscriber Line — acronim DSL sau modemurile de cablu) nu este realizabilă. MAN-urile fără fir sunt eficiente atunci când restricțiile legale fac ca instalarea sistemelor cu fir să fie imposibilă sau prea costisitoare.

Figura 1.3. Rețeaua metropolitană (MAN) fără fir constituie o alternativă pentru locuințele sau sediile de firme care doresc să se conecteze la un serviciu Internet



Performanțele MAN-urilor fără fir variază. Conexiunile între clădiri care utilizează lumina infraroșie pot atinge viteze de transmisie de 100 Gbps sau mai mult, în timp ce legăturile radio pe o distanță de aproximativ 30 de kilometri pot

realiza viteze de numai 100 Kbps. Performanțele efective depind de alegerile făcute, existând o gamă largă de tehnici și componente disponibile.

Există pe piață multe soluții brevet de MAN-uri fără fir, însă industria a început să se axeze pe utilizarea unor standarde. Unii producători utilizează standardele IEEE 802.11 ca bază pentru MAN-urile fără fir. În vreme ce folosirea sistemelor 802.11 este optimă pentru a satisface necesitățile de conectare în interiorul clădirilor, soluțiile 802.11 pot conecta clădiri pe distanțele obișnuite din interiorul orașelor utilizând antene care concentrează transmisia și recepționarea semnalelor pe o singură direcție.

Un mare număr de companii au început acum să instaleze sisteme IEEE 802.16, un standard relativ nou, cu produse care abia acum devin disponibile. 802.16 oferă soluții standardizate pentru realizarea de MAN-uri fără fir eficiente cu performanțe de ordinul megabiților pe secundă pentru raze de acțiune apreciabile. Prin urmare, 802.16 va deveni probabil un standard comun pentru MAN-urile fără fir.

Notă



În capitolul 6, intitulat *MAN-uri fără fir: rețele pentru conectarea clădirilor și a locațiilor aflate la distanță*, veți găsi detalii privitoare la tehnicile și produsele MAN-urilor fără fir.

WAN-uri fără fir

WAN-urile fără fir oferă aplicații mobile care acoperă o arie mare, cum ar fi o țară sau un continent. Un operator de telecomunicații poate face posibilă instalarea relativ scumpă a unei infrastructurii WAN fără fir pentru a oferi conectivitate pe o suprafață mare pentru o bază extinsă a unui client, datorită implicațiilor economice ale unei astfel de desfășurări. Costurile unei astfel de instalări pot fi împărțite între mai mulți utilizatori, rezultând o taxă de abonat mică.

WAN-urile fără fir, așa cum se arată în figura 1.4, ajung să aibă o acoperire aproape globală prin cooperarea mai multor companii de comunicații. Înțelegerile bine stabilite cu privire la roaming, existente între operatorii de telecomunicații permit realizarea de conexiuni continue pentru comunicații de date mobile instantanee. Plătind un furnizor de servicii de telecomunicații, un utilizator poate avea acces la servicii Internet limitate printr-o rețea WAN fără fir de aproape oriunde din lume.

004
G29



BIBLIOTECA JUDEȚEANĂ
Panait Istrati BRĂILA

618873



Despre autor

Jim Geier este fondator și consultant principal la Wireless-Nets Ltd. (www.wireless-nets.com), o firmă de consultanță independentă care acordă asistență companiilor care își dezvoltă sau își instalează produse și sisteme LAN fără fir. Experiența lui de 20 de ani cuprinde analiza, proiectarea, dezvoltarea de software, instalarea și asistența pentru numeroase sisteme de rețele client/server și de rețele fără fir pentru întreprinderi, aeroporturi, locuințe, magazine cu amănuntul, fabrici, depozite și spitale din toată lumea.

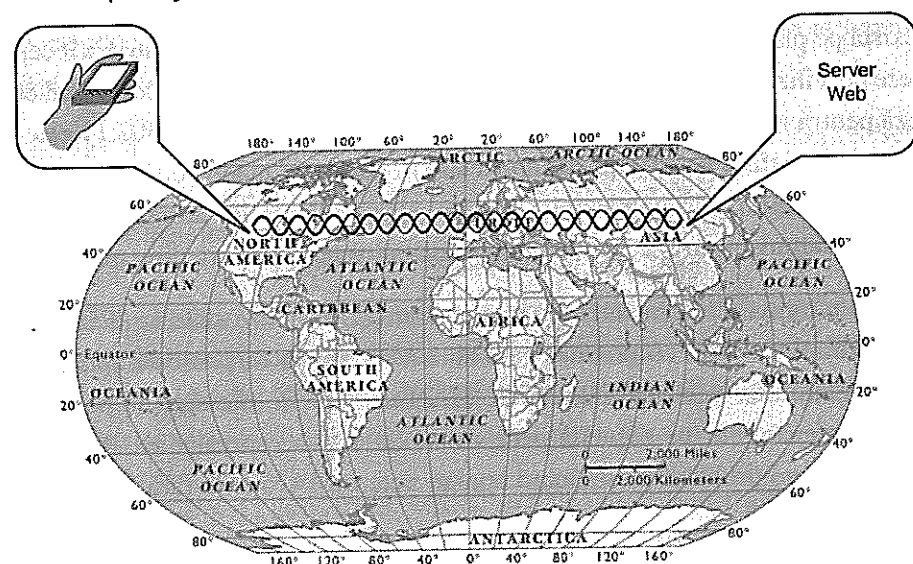
Jim este membru cu drept de vot în Wi-Fi Alliance, fiind responsabil pentru certificarea interoperabilității LAN-urilor fără fir (Wi-Fi) 802.11. A fost președinte al IEEE Computer Society, secția Dayton și președinte al Conferinței Internaționale pentru Implementarea LAN-urilor fără fir. A fost membru activ al grupului de lucru IEEE 802.11, responsabil cu dezvoltarea standardelor internaționale pentru LAN-uri fără fir. Jim este membru consultant al consiliului de administrație pentru mai multe companii de vârf din domeniul LAN-urilor fără fir.

Jim este autorul mai multor cărți, cum sunt *Wireless LANs* (publicată de editura SAM, ISBN 0672320584), *Wireless Networking Handbook* (publicată de editura MTP, ISBN 156205631X) și *Networking Reengineering* (publicată de editura McGraw-Hill, ISBN 007023034X), precum și a numeroase articole. El este redactor șef al MobilizedSoftware.com, o publicație online care oferă asistență celor care se ocupă cu implementarea aplicațiilor mobile.

Pregătirea lui Jim cuprinde o licență și un master în inginerie electrică și un master în administrarea afacerilor.

Jim Geier poate fi contactat la jimgeier@wireless-nets.com.

Figura 1.4. Rețeaua extinsă (WAN) fără fir este capabilă să asigure aplicații mobile pe o arie largă



Performanțele WAN-urilor fără fir sunt relativ scăzute, realizându-se viteze de transmisie de până la 170 Kbps, valoarea uzuală fiind 56 Kbps. Nivelul de performanță este similar cu cel al modemurilor pentru apeluri telefonice. Totuși, portaluri Web speciale, făcute pentru a optimiza fluxul de informații, lucrează în mod eficient cu dispozitive mai mici și cu rețele cu performanțe scăzute. Acest lucru conduce la obținerea maximului de performanță din lărgimea de bandă limitată oferită de WAN-urile fără fir.

Vitezele de transmisie per utilizator ale WAN-urilor fără fir sunt relativ scăzute, dar acest lucru este în general acceptabil datorită dispozitivelor mici (de exemplu, telefoane celulare sau PDA-uri) pe care oamenii le poartă cu ei în situațiile în care au nevoie de conectivitate WAN fără fir. Dimensiunile mici ale ecranelor și puterea de procesare limitată, caracteristice telefoanelor celulare, nu necesită o performanță ridicată. Transmisia video către un telefon celular mic sau către un ecran de PDA poate fi realizată cu viteze de transfer reduse.

Aplicațiile WAN fără fir presupun faptul că utilizatorii accesează Internetul, trimit și primesc e-mail-uri și accesează aplicațiile de corporație de la distanță față de locuință sau față de serviciu. De exemplu, abonații serviciilor WAN fără fir pot

sta conectați în timp ce călătoresc cu un taxi sau în timp ce se plimbă prin oraș. O rețea WAN fără fir, prin comparație cu oricare alt tip de rețea fără fir, poate ajunge în mai multe locuri, permițând utilizatorilor să-și continue activitățile legate de afaceri sau de divertisment în timp ce se află în diferite locații.

WAN-urile fără fir includ câteva standarde care evoluează lent, aflându-se în competiție. De exemplu, *Cellular Digital Packet Data (CDPD)* este o tehnică mai veche care permite transmiterea datelor prin sisteme analogice de telefonie celulară cu viteze de transfer de 19,2 Kbps. Unele companii mai oferă încă în SUA tehnica CDPD, însă aceasta devine învechită pe măsură ce operatorii de telecomunicații trec la a treia generație (3G) de sisteme de telecomunicații, care pot asigura viteze de transmisie de ordinul megabiților pe secundă.

O problemă legată de instalarea tehnicii WAN fără fir este că nu oferă posibilitatea de realizare a acoperirii în interiorul clădirilor, cum ar fi locuințele, sediile de firme, aeroporturile și centrele de afaceri. Pentru că infrastructura WAN fără fir se află afară, semnalele radio emise de aceasta pierd mare parte din puterea lor atunci când pătrund într-o clădire. Prin urmare, utilizatorii unei rețele WAN fără fir aflați în clădiri pot avea performanțe slabe sau pot chiar să nu aibă deloc asigurată conectivitatea. Unele companii de telecomunicații instalează sisteme WAN fără fir în interiorul clădirilor, însă acest lucru este costisitor și nu este realizabil în cele mai multe situații.

Notă



În capitolul 7, intitulat *WAN-uri fără fir: rețele pentru conexiuni pe tot globul*, veți găsi detalii privitoare la tehnicile și produsele WAN fără fir.

Concluzii

PAN-urile, LAN-urile, MAN-urile și WAN-urile fără fir sunt complementare și satisfac tipuri de cerințe diferite. Totuși, uneori, este dificil de distins între un anumit tip și un altul. De exemplu, o rețea LAN fără fir din interiorul unei clădiri poate asigura conectivitatea între PDA-ul unei persoane și PC-ul acesteia, asemănătoare cu cea oferită de o rețea PAN fără fir.

Totuși, tehnicile și standardele folosite diferențiază în mod clar un tip de rețea fără fir față de un altul. PAN-urile fără fir utilizează predominant IEEE 802.15 (sau Bluetooth), LAN-urile fără fir folosesc IEEE 802.11 (sau Wi-Fi) și așa mai departe.

Cuprins pe scurt

	Introducere	xv
Capitolul 1	Lumea rețelelor fără fir: o introducere în concepte	3
Capitolul 2	Arhitectura sistemului fără fir: cum funcționează rețelele fără fir	31
Capitolul 3	Fundamentele semnalelor de radiofrecvență și ale semnalelor luminoase: mediul invizibil	69
Capitolul 4	PAN-uri fără fir: rețele pentru spații restrânse	89
Capitolul 5	LAN-urile fără fir: rețele pentru clădiri și complexe de clădiri	105
Capitolul 6	MAN-urile fără fir: rețele pentru conectarea clădirilor și a locațiilor aflate la distanță	137
Capitolul 7	WAN-uri fără fir: rețele pentru conexiuni pe tot globul	151
Capitolul 8	Securitatea rețelelor fără fir: protejarea resurselor de informații	171
Anexa A	Răspunsuri la întrebările recapitulative	203
Glosar		215
Index		223

Cuprins

	Introducere	xv
Capitolul 1	Lumea rețelelor fără fir: o introducere în concepte	3
	Definirea tipurilor de rețele fără fir	3
	PAN-uri fără fir	5
	LAN-uri fără fir	7
	MAN-uri fără fir	9
	WAN-uri fără fir	11
	Concluzii	13
	Aplicațiile rețelelor fără fir	14
	Configurații de bază	14
	Accesul la Internet	15
	Transmiterea fără fir a vocii	16
	Verificarea inventarului	17
	Îngrijirea sănătății	17
	Domeniul educației	18
	Domeniul imobiliar	19
	Utilități publice	20
	Activități de teren	20
	Activități de vânzare pe teren	21
	Vânzarea prin automate	21
	Rețele publice	21
	Servicii bazate pe localizare	23
	Avantajele rețelelor fără fir	24
	Creșterea eficienței și acurateței	24
	Exemplu legat de activitatea de birou	24
	Exemplu legat de un depozit	25
	Exemplu legat de un spital	26
	Creșterea fiabilității	26
	Rezumatul capitolului	27
	Întrebări recapitulative	28

Aspectul cheie al realizării unei rețele fără fir constă în definirea completă a cerințelor sistemului și alegerea tipului de rețea care îndeplinește cel mai bine sarcina de a satisface aceste cerințe.

Din perspectiva utilizatorului, rețelele fără fir formează un amalgam. Plăcile de rețea (adaptoarele) pentru dispozitivele de calcul care pot asigura utilizarea mai multor tipuri de rețele fără fir încep să devină disponibile. Un călător, de exemplu, poate avea un telefon celular performant care posedă interfețe atât pentru LAN-uri fără fir cât și pentru WAN-uri fără fir. Acest lucru permite o conexiune fără fir similară atunci când persoana respectivă se conectează la e-mail pe baza roamingului asigurat în interiorul unui aeroport, de o rețea LAN fără fir publică, sau atunci când călătorește într-un taxi către un hotel și se conectează la un serviciu de date bazat pe sistemul celular.

Aplicațiile rețelelor fără fir

Rețelele fără fir permit realizarea multor aplicații care beneficiază de pe urma mobilității utilizatorului și a fiabilității ridicate, datorate posibilității de transmisie fără cablu, care produce mai puține erori. În plus, multe aplicații ale rețelelor fără fir realizează diminuări semnificative ale costurilor, datorită creșterii eficienței și a reducerii timpilor morți, prin comparație cu rețelele prin cablu. Majoritatea tehnicilor de rețea fără fir sunt libere de licențe, ceea ce le face să fie simple și eficiente, din punct de vedere economic, la instalare.

Configurații de bază

În cele mai multe cazuri, rețeaua fără fir este doar o extensie a unei rețele cu fir existente. În această situație, un utilizator poate realiza o anumită sarcină dintr-o locație optimă în loc să o realizeze dintr-o locație mai puțin potrivită. De exemplu, un funcționar care descarcă un camion poate folosi un dispozitiv de mână fără fir pentru a scana obiectele pe care le coboară din mașină. Acest lucru este mult mai eficient decât scrierea pe hârtie a codurilor obiectelor pentru ca acestea să fie apoi introduse printr-un terminal aflat undeva în clădire, departe de rampa de descărcare.

Alte situații presupun folosirea de rețele fără fir dedicate, care elimină complet nevoia de cabluri. De exemplu, o echipă de intervenție pentru cazuri de urgență, care este responsabilă de locul prăbușirii unui avion, poate stabili cu rapiditate o rețea fără fir temporară, în zona din imediata vecinătate. Toate dispozitivele de calcul comunică

direct între ele. Acest lucru face posibil ca membrii echipei să aibă acces centralizat la datele importante privitoare la accident.

Aplicațiile rețelelor fără fir pot ține atât de domeniul public cât și de cel privat. O companie sau proprietarul unei locuințe care cumpără și instalează o rețea fără fir pentru uzul propriu realizează o aplicație privată. De regulă, aplicațiile private sunt făcute pentru a fi disponibile doar pentru angajații companiei respective sau pentru locuitorii casei respective. Accesul publicului larg la aceste aplicații nu este permis. De fapt, în general, companiile implementează măsuri de securitate pentru a se asigura că numai persoanele autorizate se pot conecta la rețea pentru a accesa serviciile.

Aplicațiile publice, pe de altă parte, asigură acces liber pentru oricine. De exemplu, o persoană care călătorește pentru afaceri poate utiliza o LAN fără fir publică dintr-un aeroport pentru a accesa Internetul în timp ce așteaptă avionul. Aceste „puncte fierbinți” au devenit disponibile pe scară largă în aeroporturi și în alte arii, cum ar fi hotelurile, centrele de afaceri și cafenelele, unde se produc aglomerări de persoane care posedă dispozitive de calcul.

Accesul la Internet

Unul dintre motivele cele mai convingătoare pentru instalarea unei rețele fără fir este posibilitatea de partajare a unei conexiuni Internet cu mare viteză de transmisie. În cazul acestui tip de configurație, fiecare membru al unei familii sau fiecare angajat al unei firme mici poate partaja cu ușurință o unică conexiune de mare viteză, asigurată de un modem de cablu sau de un modem DSL. Acest lucru este convenabil și realizează economii pentru că toată lumea poate avea acces simultan la Internet, deplasându-se peste tot prin casă sau prin sediul firmei.

De asemenea, rețeaua fără fir din acest scenariu crește flexibilitatea rețelei pentru că este ușor să se adauge noi stații de lucru în orice moment, fără să fie necesară instalarea de cabluri. Repoziționarea PC-urilor conectate fără fir, ca și cea a imprimantelor sau a serverelor, este și aceasta realizabilă fără probleme.

O companie poate implementa o rețea fără fir pentru a asigura posibilitatea ca angajați care vizitează sediul sau oaspeții care posedă dispozitive de calcul fără fir să se poată conecta rapid la rețea, pentru aceasta fiind necesare un minim de configurații. Capacitatea de a utiliza Internetul de la distanță față de casă poate crește mult productivitatea. Vizitatorul poate să-și pornească doar laptopul și astfel să aibă instantaneu acces la e-mail și la aplicații.

Capitolul 2 Arhitectura sistemului fără fir:

cum funcționează rețelele fără fir	31
Componentele sistemului rețelei fără fir	31
Utilizatori	32
Dispozitive de calcul	33
Plăci interfață de rețea (plăci de rețea — NIC-uri)	34
Mediul aerian	37
Infrastructuri de rețele fără fir	38
Stații de bază	38
Controlere de acces	40
Software pentru conectivitatea aplicațiilor	42
Sistemul de distribuție	46
Sistemele de administrare	48
Protecție/securitate	48
Asistența la birou	49
Managementul configurației	49
Monitorizarea rețelei	50
Raportarea	50
Reproiectarea	51
Întreținerea	51
Arhitectura rețelei fără fir	52
Semnalele care transmit informația	54
Semnalele digitale	54
Semnalele analogice	56
Fluxul de informații printr-o rețea fără fir	57
Punctele finale ale fluxului de informații	57
Introducerea, stocarea și afișarea informațiilor	58
Legătura cu mediul aerian	58
Accesul la mediu	59
Controlul erorilor	61
Transferul, fără fir al semnalelor purtătoare de date	65
Conectarea la infrastructura rețelei fără fir	65
Rezumatul capitolului	66
Întrebări recapitulative	67

Capitolul 3 Fundamentele semnalelor de radiofrecvență și ale

semnalelor luminoase: mediul invizibil	69
Transceiverele fără fir	69
Semnalele de radiofrecvență (RF)	70
Caracteristicile semnalelor RF	70
Pro și contra semnalelor RF	72
Distorsionarea semnalelor RF	73
Interferența	73
Propagarea pe mai multe căi	74
Semnalele luminoase	76
Caracteristicile semnalelor luminoase	76
Pro și contra semnalelor luminoase	78
Distorsionarea semnalelor luminoase	78
Interferența	79
Atenuarea produsă de obstacole sau de condițiile meteo	79
Modularea: pregătirea semnalelor pentru propagare	80
Modularea în frecvență (FSK)	81
Modularea în fază (PSK)	82
Modularea în fază și amplitudine (QAM)	82
Modularea în spectru larg	83
Multiplexarea prin divizarea ortogonală a frecvenței	85
Modularea în bandă ultra-largă	86
Rezumatul capitolului	87
Întrebări recapitulative	87

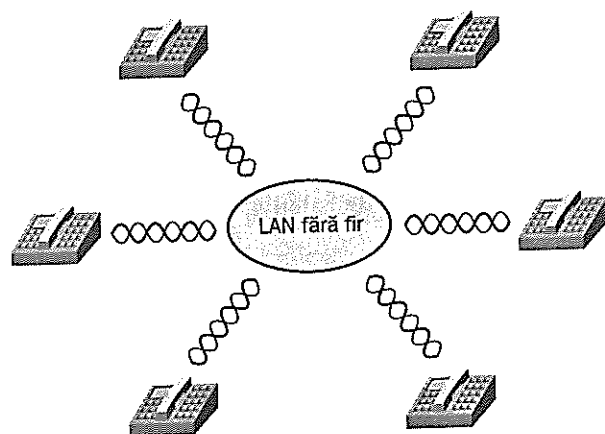
Capitolul 4 PAN-uri fără fir: rețele pentru spații restrânse

Componente PAN fără fir	89
Dispozitive pentru utilizator	89
NIC-uri radio	90
Adaptoare USB	90
Routere	91
Sisteme PAN fără fir	91
Sisteme pentru locuințe și sedii mici	92
Sincronizarea	92
Fluxul continuu de multimedia	92
Legătura cu perifericele	93

Transmiterea fără fir a vocii

Utilizarea rețelor fără fir pentru a asigura transmisia conversațiilor este o soluție avantajoasă atunci când oamenii au nevoie permanent să stea în contact unii cu alții. De fapt, o rețea LAN fără fir proiectată să asigure comunicațiile prin voce poate înlocui complet sistemul tradițional de telefonie prin fir dintr-o clădire (vezi figura 1.5). Combinația realizată prin transmisia vocii și a datelor prin aceeași rețea fără fir asigură mobilitate totală și costuri scăzute de operare.

Figura 1.5. O rețea LAN fără fir care oferă infrastructura pentru un sistem de telefonie din interiorul unei clădiri



De exemplu, angajații unui magazin de vânzare cu amănuntul pot localiza anumite obiecte de îmbrăcăminte pentru un client sau pot verifica inventarul utilizând telefoane speciale bazate pe o rețea LAN fără fir. LAN-ul fără fir dintr-un magazin poate să asigure și transmisia codurilor de bare atunci când se fac inventarele sau se stabilesc prețurile, folosind un scanner de mână fără fir pentru codurile de bare. De aici rezultă scăderi de costuri pentru că firma respectivă trebuie să instaleze și să întrețină un singur sistem de comunicații care transportă atât vocea cât și datele.

Tot așa, o firmă poate să-și desfășoare întregul sistem telefonic printr-o rețea LAN fără fir. Acest lucru permite angajaților să poarte în permanență telefoanele cu ei, ca și cum ar fi telefoane celulare standard. Angajații vor putea accepta apeluri din interiorul firmei, în orice moment, folosind un singur telefon.

Verificarea inventarului

Multe firme beneficiază de pe urma utilizării LAN-urilor fără fir atunci când își administrează procesul de fabricație. Acest lucru micșorează costurile de operare. Deoarece conexiunile dintre echipamentele de producție și sistemul central de control sunt realizate fără fir, compania poate reconfigura procesul de asamblare în orice moment, de oriunde, economisind timp și bani.

Prin utilizarea unei LAN fără fir, o companie poate urmări și actualiza inventarul în timp real, asigurând o creștere spectaculoasă a eficienței și a preciziei. În domeniul comerțului cu amănuntul, îndată ce un funcționar cumpără sau stochează un produs, o soluție de management fără fir poate actualiza inventarul. În cazul proceselor de producție, compania respectivă poate ține la zi evidența materiilor prime și a produselor finite. Angajații echipați cu scanere de coduri de bare fără fir pot verifica sau schimba prețurile produselor sau pot verifica cantitățile din stoc.

Îmbunătățirea preciziei asigurată de utilizarea unei LAN fără fir în administrarea inventarelor generează o reacție în lanț de apariție a unor beneficii. Pentru că funcționarii introduc informațiile direct în calculatorul central prin intermediul scanerelor de mână, nu mai este necesară completarea și administrarea hârtiilor. Acest lucru reduce semnificativ erorile umane legate de introducerea datelor, ceea ce conduce la înregistrări contabile exacte, fapt important pentru companiile de producție, deoarece înregistrările contabile exacte conduc la plata unor impozite corecte, iar penalizările (și posibilele probleme legale) sunt menținute la un minim.

Îngrijirea sănătății

Din ce în ce mai multe spitale își instalează rețele fără fir pentru a îmbunătăți eficiența activității și confortul. În majoritatea cazurilor, spitalele instalează LAN-uri fără fir în zonele cu trafic mărit de pacienți, incluzând sălile de urgențe, secțiile de terapie intensivă, sălile de tratament, precum și birourile medicilor și sălile de așteptare pentru pacienți. Personalul spitalului poate utiliza dispozitive de calcul mobile pentru a crește eficiența și acuratețea îngrijirii bolnavilor.

Centrele de îngrijire a sănătății trebuie să păstreze înregistrări exacte pentru a asigura o îngrijire de calitate a pacienților. O greșală banală poate costa viața cuiva. Prin urmare, medicii și asistentele trebuie să înregistreze cu atenție rezultatele analizelor,

Tipărirea	93
Legăturile la Internet	94
Întreprinderi	94
Tehnici PAN fără fir	95
802.15	95
Bluetooth	96
Caracteristicile de bază	96
Va putea Bluetooth să înlocuiască LAN-urile fără fir?	97
Vor putea LAN-urile fără fir să înlocuiască Bluetooth?	97
Minimizarea interferențelor Bluetooth	98
IrDA	101
Caracteristicile de bază	101
Rezumatul capitolului	102
Întrebări recapitulative	103

Capitolul 5	LAN-urile fără fir: rețele pentru clădiri și complexe de clădiri	105
	Componente LAN fără fir	105
	Dispozitive pentru utilizator	105
	NIC-uri radio	106
	Puncte de acces	106
	Routere	108
	Repetoare	109
	Antene	110
	Sisteme LAN fără fir	110
	LAN-uri fără fir pentru locuințe și sedii de firme mici	111
	LAN-uri fără fir pentru întreprinderi (pentru sedii de firme mari)	112
	LAN-uri fără fir publice	114
	LAN-uri fără fir ad-hoc	117
	Tehnici LAN fără fir	117
	802.11	118
	Stratul MAC 802.11	118
	Straturile fizice 802.11	124
	Wi-Fi	130
	Ce înseamnă certificarea Wi-Fi	130

Accesul protejat Wi-Fi	131
HiperLAN/2	131
Îmbunătățirile aduse de HiperLAN/2	132
Constituie sistemele HiperLAN/2 o amenințare pentru sistemele 802.11?	133
Rezumatul capitolului	134
Întrebări recapitulative	134

Capitolul 6	MAN-urile fără fir: rețele pentru conectarea clădirilor și a locațiilor aflate la distanță	137
	Componente MAN fără fir	138
	Punți	138
	Punți contra puncte de acces	139
	Punți de bază pentru conectare Ethernet-la-rețea-fără-fir ..	139
	Punți grup de lucru	140
	Antene direcționale	140
	Antene semidirecționale	141
	Antene de mare directivitate	141
	Efectul de polarizare	142
	Sisteme MAN fără fir	142
	Sisteme punct-la-punct	142
	Sisteme punct-la-multe-puncte	143
	Sisteme radio cu pachete de date	144
	Tehnici MAN fără fir	145
	802.11 și Wi-Fi	145
	802.16	146
	Rezumatul capitolului	147
	Întrebări recapitulative	148

Capitolul 7	WAN-uri fără fir: rețele pentru conexiuni pe tot globul ...	151
	Componente WAN fără fir	152
	Dispozitive pentru utilizatorii de WAN-uri fără fir	152
	NIC-uri radio	153
	Stații de bază	154
	Antene	155

datele fizice, rețetele de medicamente și procedurile chirurgicale. Adesea, înregistrarea acestor lucruri pe hârtie copleșește personalul medical, ocupând 50-70% din timpul de lucru. Utilizarea unor dispozitive mobile pentru colectarea datelor, care apoi sunt transmise fără a uza de fire, către o bază de date centralizată, conduce la o creștere semnificativă a acurateții datelor și la sporirea gradului lor de accesibilitate pentru cei care au nevoie de informații.

De asemenea, medicii și asistentele medicale sunt extrem de mobili, trecând de la o încăpăre la alta pentru a se ocupa de pacienți. Utilizarea înregistrărilor electronice privitoare la pacienți, împreună cu capacitatea de a introduce, vizualiza și actualiza datele pacienților de oriunde din cadrul spitalului, cresc acuratețea și viteza actului medical. Această îmbunătățire este posibilă punând la dispoziția fiecărei asistente medicale și a fiecărui medic, câte un dispozitiv de înregistrare a datelor cu creion electronic, cum ar fi o tabletă digitală¹ sau un PDA, cuplată printr-o rețea fără fir la o bază de date care stochează informațiile medicale critice privitoare la pacienți.

Un medic care se ocupă de un pacient din spital, de exemplu, poate trimite o comandă pentru o analiză a sângelui prin introducerea solicitării într-un calculator de mână. Laboratorul primește comanda pe cale electronică și trimite un laborant să preia sângele de la pacient. Laboratorul efectuează analizele solicitate de către medic și introduce rezultatele în fișa medicală electronică a pacientului. Medicul poate verifica ulterior rezultatele prin intermediul calculatorului de mână, de oriunde s-ar afla în spital.

O altă aplicație spitalicească este urmărirea produselor farmaceutice. Utilizarea unui dispozitiv de mână mobil care scanează și tipărește coduri de bare crește în mod spectaculos eficiența și acuratețea operațiunilor cu produsele farmaceutice, cum ar fi recepționarea, distribuirea, prepararea și inventarierea acestora precum și urmărirea datelor de expirare. Totuși, cel mai important lucru este să se asigure posibilitatea ca personalul medical să poată administra medicamentul adecvat pacientului care are nevoie de acesta, la momentul oportun.

Domeniul educației

Multe licee și multe școli elementare găsesc că există avantaje în a instala LAN-uri fără fir, mai ales pentru a asigura elevilor lor aplicații de rețea mobile. De fapt, școlile au început să folosească accesul la o rețea LAN fără fir ca pe un avantaj în

¹ Dispozitiv de introducere a datelor, constând dintr-o tabletă electronică și un cursor sau stilou cu ajutorul cărora se realizează introducerea datelor (n.tr.).

competiția în care sunt angajate. Aceste școli își îndreaptă atenția către numărul tot mai mare de elevi posesori de laptopuri care își manifestă dorința de a accesa Internetul și resursele școlii de oriunde din campus, cum ar fi din clase, din biblioteci și din dormitoare. Elevii au astfel posibilitatea de a-și verifica cu promptitudine e-mail-ul, pot naviga pe Web, pot accesa aplicații școlare specializate, își pot vizualiza calificativele și își pot verifica foaia matricolă. Ca urmare, elevii își folosesc mai bine timpul de lucru.

Instalarea și întreținerea unor săli cu calculatoare pentru ca elevi să acceseze Internetul și să-și poată face temele sunt costisitoare. Elevii sunt deseori nevoiți să aștepte pentru a putea utiliza un calculator dintr-o astfel de sală, ceea ce presupune întreruperi în activitățile acestora. O rețea LAN fără fir, însă, oferă elevilor acces la resursele dorite folosind laptopul propriu, de oriunde din campus și la orice moment, chiar și după ce programul sălii tradiționale de calculatoare a luat sfârșit. Acest lucru asigură un acces la rețea mai bine distribuit al tuturor elevilor, crescând eficiența activității acestora. Desigur că, în aceste condiții, școala va economisi și banii necesari funcționării sălii cu calculatoare.

Domeniul imobiliar

Cei care lucrează în vânzări, în domeniul imobiliar, își efectuează mare parte din muncă în afara biroului, de obicei discutând cu clienții la locul proprietății care este vândută sau închiriată. Înainte de a pleca de la birou, de regulă, persoanele care lucrează în vânzări identifică locațiile care urmează să fie prezentate clientului, tipăresc informațiile privitoare la proprietățile respective și apoi se deplasează cu mașina la fiecare locație, împreună cu potențialul cumpărător. Dacă clientul nu este mulțumit de nici una dintre proprietăți, agentul imobiliar trebuie să se întoarcă la birou și să găsească noi oferte. Chiar dacă clientul se decide să cumpere o proprietate, vor trebui să se deplaseze împreună înapoi la sediul agenției imobiliare pentru a întocmi actele de vânzare.

Rețelele fără fir fac ca activitatea de vânzare din domeniul imobiliar să devină mult mai eficientă. Agentul imobiliar aflat pe teren poate utiliza un calculator pentru a accesa informații privitoare la diverse proprietăți. De asemenea, agentul poate folosi un calculator și o imprimantă portabile pentru a produce, la punctul de vânzare, contractele și actele de împrumut necesare, care trebuie să fie semnate.

Sisteme WAN fără fir	156
WAN-uri fără fir pe bază de rețele celulare	157
Prima generație de sisteme celulare	158
A doua generație de sisteme celulare	158
A treia generație de sisteme celulare	159
WAN-uri fără fir bazate pe spațiu	161
Sateliți	161
Comunicații bazate pe arderea meteorilor în atmosfera terestră	164
Tehnici WAN fără fir	165
Accesul multiplu prin divizarea spectrului de frecvențe	165
Accesul multiplu prin divizarea timpului de transmisie	166
Accesul multiplu cu divizare prin cod	166
Accesul multiplu prin divizare spațială	167
Rezumatul capitolului	167
Întrebări recapitulative	168

Capitolul 8	Securitatea rețelelor fără fir: protejarea resurselor de informații	171
	Amenințările la adresa securității rețelelor	171
	Monitorizarea traficului	172
	Accesul neautorizat	172
	Atacuri de tipul omul-la-mijloc	174
	Negare de serviciu	176
	Criptarea	178
	Criptarea WEP	181
	Funcționarea criptării WEP	181
	Dezavantajele criptării WEP	182
	Când trebuie folosită criptarea WEP	183
	Protocolul de integritate cu cheie temporară	183
	Accesul protejat Wi-Fi	184
	Rețele private virtuale	185
	Autentificarea	185
	Punctele vulnerabile ale autentificării 802.11	185
	Filtrele MAC	187

Autentificarea prin folosirea criptării cu cheie publică	187
Standardul 802.1x	188
Funcționarea 802.1x	188
Tipuri de autentificare	190
Politici de securitate	190
Etapile de evaluare a securității rețelei	191
Revizuirea politicilor de securitate existente	191
Revizuirea sistemului existent	192
Discuțiile cu utilizatorii	192
Verificarea configurațiilor dispozitivelor fără fir	192
Identificarea stațiilor de bază pirat	193
Realizarea de teste de penetrare	194
Analiza lacunelor sistemului de securitate	194
Recomandarea de îmbunătățiri aduse securității	194
Politici de securitate uzuale	195
Plasarea utilizatorilor fără fir în exteriorul unui parafoc ...	195
Utilizarea unei criptări eficiente	195
Asigurați-vă că software-ul și hardware-ul sunt actualizate	196
Protejarea fizică a stațiilor de bază	196
Atribuiți parole puternice pentru stațiile de bază	197
Evitați difuzarea SSID-urilor	197
Limitarea propagării undelor radio	197
Implementarea de parafocuri personale	198
Monitorizarea configurației stațiilor de bază	198
Desfășurarea de controale	198
Rezumatul capitolului	199
Întrebări recapitulative	199

Anexa A	Răspunsuri la întrebările recapitulative	203
----------------	---	------------

Glosar	215
---------------------	------------

Index	223
--------------------	------------

Utilități publice

Companiile care furnizează utilitățile folosesc și întrețin un sistem extrem de întins care livrează energia și gazele naturale către industrii și locuințe. Aceste companii trebuie să monitorizeze în permanență funcționarea sistemului de distribuție a energiei electrice, rețeaua de gaze și pe cea de apă și trebuie să verifice consumurile, cel puțin o dată pe lună, pentru a putea calcula facturile. În mod tradițional, acest lucru este realizat de către o persoană care trece pe la fiecare locație, vizitând locuințele și sediile companiilor, înregistrează informațiile și apoi introduce datele într-un calculator aflat la sediul companiei care furnizează utilitățile.

Astăzi, aceste companii folosesc WAN-uri fără fir pentru a asigura citirea automatizată a consumurilor și monitorizarea sistemelor. În locul persoanei care citește contoarele, înregistrează informațiile pe hârtie, pentru a le introduce ulterior într-un calculator, pentru procesare, contoarele pot transmite periodic datele, printr-o rețea WAN fără fir, la sediul companiei care furnizează utilitățile. Acest lucru economisește timp și reduce costurile suplimentare prin eliminarea necesității existenței unui cititor de contoare uman.

Activități de teren

Personalul care efectuează activități de teren petrece cea mai mare parte din timp călătorind pentru a instala sau întreține sisteme sau pentru a inspecta locații aflate în construcție. Pentru a-și îndeplini sarcinile, aceste persoane trebuie să aibă acces la documentațiile de produse și la proceduri. În mod tradițional, angajații cu muncă de teren trebuie să poarte după ei cantități mari de documentație, la locații unde adesea nu există telefoane, ori nici chiar electricitate.

În unele cazuri, angajatul cu muncă de teren nu poate lua cu el, la o locație, toată documentația, ceea ce produce întârzieri în obținerea informațiilor. De asemenea, în cazul călătoriilor lungi, este posibil ca informația să nu mai fie de actualitate. Livrarea actualizărilor solicitate poate dura zile întregi pentru a ajunge la persoana aflată în teren. Accesul la documentație pe baza unei rețele WAN fără fir poate, fără îndoială, să îmbunătățească activitatea de teren. De exemplu, un angajat cu muncă de teren poate duce cu el un calculator portabil conectat la LAN-ul de la sediu, care conține documentația corectă pentru toate informațiile necesare.

Activități de vânzare pe teren

Profesioniștii din vânzări sunt în continuă mișcare pentru a-și întâlni clienții. Aflată la o locație cu un client, o astfel de persoană are nevoie să acceseze mari cantități de informații care descriu produse și servicii. De asemenea, aceste persoane trebuie să transmită comenzi, să trimită situații diverse — cum ar fi programări de întâlniri — la sediul central sau să țină inventarul produselor.

Pe baza accesului fără fir la rețeaua principală de la sediu, o persoană din vânzări poate vizualiza informații centralizate de contact, poate prelua informații legate de produse, poate înainta propuneri, poate edita contracte și poate menține contactul cu ceilalți angajați din sediu sau cu alte persoane care lucrează în vânzări. Acest contact permite celor din vânzări să încheie procesul de vânzare direct din locația unde se află clientul, crescând astfel șansele de a se realiza o vânzare de succes și scurtând ciclul acestui proces.

Vânzarea prin automate

Companiile de băuturi și de gustări plasează automate în hoteluri, aeroporturi și sedii de firme pentru a crește vânzările produselor lor. Automatele elimină necesitatea existenței unui vânzător. Totuși, aceste companii trebuie să trimită angajați în teren pentru a aproviziona periodic automatele. În anumite situații, automatele pot să se golească înainte ca să se petreacă aprovizionarea, pentru că firmele nu au cum să afle că un anumit produs s-a consumat.

O rețea WAN fără fir poate asigura monitorizarea nivelului stocurilor prin transferarea datelor adecvate de la fiecare dintre automate către o bază de date centralizată, care poate fi urmărită cu ușurință de personalul din sediul companiei. O asemenea monitorizare permite companiei să acționeze în avans pentru aprovizionarea automatelor, deoarece sunt cunoscute în permanență nivelurile stocurilor din fiecare automat. Acest lucru permite realizarea unei programări adecvate a activității de aprovizionare efectuate de personalul care se deplasează pentru a reface stocurile.

Rețele publice

Datorită creșterii semnificative a numărului de laptopuri, PDA-uri și telefoane celulare operaționale, apare o nevoie din ce în ce mai mare de a exista interfețele mobile de acces la Internet și la aplicațiile de corporație. Utilizatorii doresc, și se

Introducere

De câteva zeci de ani, oamenii folosesc rețelele de calculatoare pentru a interconecta calculatoare personale (PC-uri) și servere în firme, universități și orașe. Însă, a avut loc o evoluție în direcția folosirii rețelelor fără fir. De fapt, în prezent, sunt disponibile interfețe fără fir pentru utilizarea serviciilor de rețea care ne permit să folosim poșta electronică și aplicații de acces și să navigăm pe Internet aproape din orice loc ne-am afla.

Aceste aplicații fără fir le-au oferit oamenilor posibilitatea de a-și extinde locul de muncă într-un mod care produce beneficii semnificative. Cei care călătoresc pentru afaceri, de exemplu, pot răspunde la mesajele e-mail în timp ce așteaptă decolarea avionului, pe aeroport. Proprietarul unei locuințe poate să partajeze cu ușurință o conexiune comună la Internet între mai multe PC-uri și laptopuri, fără să instaleze cabluri. Această carte explică tehnicile de bază care fac ca aceste tipuri de aplicații să poată fi realizate.

Scopurile acestei cărți

Intenția acestei cărți este să ofere o introducere de bază în domeniul aplicațiilor, componentelor și tehnicilor pentru rețelele fără fir. Aceste concepte oferă o bază solidă pentru înțelegerea, mai detaliată, a diverselor subiecte referitoare la rețelele fără fir. După ce veți citi această carte, veți putea să continuați, în mod eficient, studiarea unor rețele fără fir specifice.

Cui îi este adresată această carte

Cartea de față a fost scrisă pentru orice persoană care începe să studieze rețelele fără fir. Nu este necesar ca cititorii să posede cunoștințe tehnice. Directorii, administratorii și patronii de firme vor beneficia de pe urma citirii acestei cărți, la fel ca și inginerii sau tehnicienii. Chiar și utilizatorii obișnuiți care doresc să înțeleagă funcționarea internă a rețelelor fără fir, vor găsi această carte interesantă.

așteaptă să li se ofere, conectivitate mobilă constantă și directă către toate sursele de informații, la un nivel înalt de performanță și de disponibilitate. Rețelele fără fir oferă infrastructura necesară pentru asigurarea solicitărilor existente în spațiile publice care se află la distanță de locuințe sau de servicii.

O rețea fără fir publică oferă modalitatea prin care oamenii se pot conecta la Internet. În general, locurile în care se află grupuri mari de oameni, care au nevoie sau doresc conexiuni la rețea, oferă acces la LAN-uri fără fir. Pe de altă parte, MAN-uri sau WAN-uri fără fir realizează acoperirea unor arii mai largi, cu o populație distribuită ici și colo.

LAN-urile fără fir publice sunt întâlnite în locuri comune cum ar fi hotelurile și restaurantele, însă există și alte tipuri de locații care au instalate LAN-uri fără fir pentru acces public. De exemplu, aproximativ 90% dintre proprietarii de ambarcațiuni utilizează Internetul, cu regularitate, atunci când se află acasă sau la birou. Mulți dintre aceștia doresc să aibă acces la Internet atunci când se relaxează pe ambarcațiunile lor, mai ales atunci când acestea se află la chei, în porturi. Prin urmare, porturile de pe tot globul își instalează LAN-uri fără fir pentru a oferi navigatorilor acces la aplicații Internet.



Notă

Puteți găsi o listă cuprinzătoare de LAN-uri fără fir publice pe site-ul Web <http://www.wi-fihotspotlist.com/>.

Pentru a folosi o rețea LAN fără fir publică, utilizatorii trebuie să aibă un dispozitiv de calcul, cum ar fi un laptop, cu o placă de rețea LAN fără fir. IEEE 802.1b (Wi-Fi) este cel mai comun tip de LAN fără fir instalat astăzi de către furnizorii de rețele fără fir publice. Placa de rețea a dispozitivului de calcul sesizează, în mod automat, prezența unei LAN fără fir și se conectează la rețea. Înainte de a accesa Internetul, utilizatorul trebuie să se aboneze la serviciu respectiv, în general prin intermediul unui site Web accesibil din LAN-ul fără fir. Unele LAN-uri fără fir publice oferă accesul gratuit, însă majoritatea furnizorilor taxează un preț nominal pentru utilizarea serviciului.

O altă formă de rețea fără fir publică utilizează tehnici MAN fără fir pentru a furniza legături de comunicații fără fir între abonați (locuințe sau sedii de firme) și Internet. Furnizorul instalează o mică antenă parabolică pe clădirea respectivă (locuință sau sediu de firmă) și o îndreaptă către un distribuitor centralizat. Acest sistem punct-la-multipunct oferă conexiunea finală necesară furnizării accesului la Internet pentru o locație la care conexiunile prin modemuri de cablu sau prin modemuri DSL nu sunt disponibile sau nu sunt realizabile.

Servicii bazate pe localizare

Prin intermediul rețelelor fără fir, puteți face ca poziția unei anumite persoane sau a unui anumit obiect să fie cunoscută la o locație centrală. Capacitatea de a urmări poziția unor obiecte în mișcare aduce cu sine posibilitatea realizării unor aplicații interesante. Coordonatele utilizatorilor pot fi încărcate într-o aplicație bazată pe server care implementează un serviciu bazat pe localizare.

De exemplu, un furnizor de LAN-uri fără fir publice poate folosi acest concept pentru a afișa informații pertinente pentru călătorii care trec printr-un aeroport sau printr-o gară. Informațiile pot include poziția acestora pe o hartă în mișcare, într-o modalitate pe care pasagerii o pot utiliza pentru a găsi calea către următoarea poartă de plecare sau către cel mai apropiat restaurant. Valoarea acestui serviciu bazat pe localizare constă în aceea că poate îndrepta pasagerii către un anumit loc de întâlnire.

Un spital poate utiliza *servicii bazate pe localizare* pentru a determina poziția doctorilor sau a asistentelor medicale. Acest lucru permite administrației spitalului să trimită persoana potrivită la o urgență. Pacienții vor beneficia de o îngrijire mai rapidă și mai eficientă.

Utilizarea unui sistem care identifică locațiile prin intermediul LAN-urilor fără fir tinde să răspundă așteptărilor consumatorilor. De exemplu, capacitatea de a localiza copiii este extrem de valoroasă. Imaginați-vă un parc de distracții și un copil mic care hoinărește prin acesta fără știința părinților. Folosind un sistem de localizare, părinții îl pot găsi cu ușurință pe micul hoinar într-o mulțime de oameni. Un emițător fără fir pentru urmărire, mascat în hainele copilului, face ca acest sistem să poată constitui un ajutor neprețuit în cazul în care cineva răpește copilul.

Un complex comercial mare poate instala un sistem de localizare și poate transmite mesaje publicitare clienților care posedă PDA-uri. Sistemul ia în considerație poziția fizică a cumpărătorilor în complex și personalizează conținutul efectiv al mesajului în mod corespunzător. Cumpărătorii pot să-și folosească mai bine timpul pe care îl au la dispoziție, iar magazinele vor vinde mai bine.

Utilizatorii din acest exemplu pot recepționa un mesaj electronic conținând și o hartă pe PDA-urile lor fără fir, după ce au intrat în complexul comercial. Harta identifică poziția exactă a cumpărătorului în cadrul complexului. Dacă persoana respectivă execută un clic pe un magazin, o toaletă sau un bancomat, harta va indica traseul care trebuie urmat până la locația dorită. Dacă soțul, respectiv soția sau un prieten de cumpărături posedă și acesta un dispozitiv fără fir, lucrul acesta permite localizarea reciprocă a partenerilor.

Cum este organizată această carte

Această carte acoperă toate aspectele referitoare la rețelele fără fir, punând accentul pe caracteristicile specifice ale sistemelor fără fir. Primele trei capitole furnizează conceptele de bază pentru o mai bună înțelegere a diverselor tipuri de rețele fără fir pe care le descriu capitolele care urmează. Ultimul capitol oferă detalii privitoare la securitatea (protecția) rețelelor fără fir.

- **Capitolul 1 „Lumea rețelelor fără fir: o introducere în concepte”** — Definiște pe larg conceptul de rețea fără fir și pe scurt diversele tipuri de rețele fără fir. Sunt date mai multe exemple de aplicații de rețele fără fir, prezentându-se beneficiile obținute prin folosirea acestora.
- **Capitolul 2 „Arhitectura sistemului fără fir: cum funcționează rețelele fără fir”** — Oferă explicații cuprinzătoare referitoare la diversele componente ale unei rețele fără fir. Prin ilustrarea felului în care fluxul de informații parcurge rețeaua, acest capitol oferă o bază excelentă pentru înțelegerea modului de funcționare a diverselor tipuri de rețele fără fir.
- **Capitolul 3 „Fundamentele semnalelor de radiofrecvență și ale semnalelor luminoase: mediul invizibil”** — Descrie detaliat modul în care este purtată informația, de către semnalele de radio frecvență și semnalele luminoase, prin mediul aerian. Acestea sunt elementele primare care definesc o rețea fără fir.
- **Capitolul 4 „PAN-uri fără fir: rețele pentru spații restrânse”** — Explică componentele, tehnicile și configurațiile folosite pentru rețelele fără fir personale (PAN-uri).
- **Capitolul 5 „LAN-urile fără fir: rețele pentru clădiri și complexe de clădiri”** — Explică componentele, tehnicile și configurațiile folosite pentru rețelele fără fir locale (LAN-uri).
- **Capitolul 6 „MAN-urile fără fir: rețele pentru conectarea clădirilor și a locațiilor aflate la distanță”** — Explică componentele, tehnicile și configurațiile folosite pentru rețelele fără fir metropolitane (MAN-uri).
- **Capitolul 7 „WAN-uri fără fir: rețele pentru conexiuni pe tot globul”** — Explică componentele, tehnicile și configurațiile folosite pentru rețelele fără fir extinse (WAN-uri).

- **Capitolul 8 „Securitatea rețelelor fără fir: protejarea resurselor de informații”** — Descrie amenințările potențiale la adresa securității rețelelor fără fir și măsurile care pot fi luate. Atunci când instalați o rețea fără fir, securitatea este importantă datorită naturii semnalelor fără fir.
- **Anexa A „Răspunsuri la întrebările recapitulative”** — Conține răspunsurile și explicațiile referitoare la întrebările recapitulative de la sfârșitul fiecărui capitol.
- **Glosar** — Glosarul este un instrument pe care îl puteți folosi cu ușurință pentru a afla definițiile termenilor cheie utilizați pe parcursul acestei cărți.

Cum sunt structurate capitolele

Această carte posedă câteva caracteristici care vă pot ajuta să asimilați subiectele referitoare la rețelele fără fir. Iată o descriere sumară a acestor elemente:

- **Obiectivele capitolului** — Fiecare capitol începe cu o listă de obiective care vor fi abordate și care rezumă ce veți învăța pe parcursul capitolului.
- **Evidențieri de termeni cheie și Glosarul** — Pe parcursul capitolelor, veți vedea termeni evidențiați prin litere aldine și cursive. Aceștia sunt termenii mai importanți din domeniul rețelelor. De aceea, dacă nu sunteți familiarizat cu un astfel de termen sau dacă aveți nevoie să vă reîmprospătați memoria în privința acestor termeni, vă puteți uita în Glosarul de la sfârșitul cărții unde veți găsi definiții complete.
- **Rezumatul capitolului** — În fiecare capitol sunt trase concluziile într-o secțiune cuprinzătoare numită *Rezumatul capitolului* care revede obiectivele capitolului, realizând astfel o completare a explicațiilor și discutând relațiile cu următoarele capitole.
- **Întrebările recapitulative** — Fiecare capitol se încheie cu niște întrebări recapitulative. Aceste întrebări testează asimilarea ideilor și conceptelor de bază descrise în capitolul respectiv. Răspunsurile la aceste întrebări le puteți găsi în Anexa A.

Avantajele rețelelor fără fir

Oamenii din toată lumea află despre avantajele oferite de conectivitatea fără fir la verificarea e-mail-ului, la navigarea pe Internet și la accesarea aplicațiilor de corporație. Îmbunătățirea continuă a produselor care includ interfețe fără fir permit acestor oameni să renunțe la conectivitatea prin fir și să profite de avantajele oferite, de mobilitate și de flexibilitate. Rezultatul constă în o mai mare eficiență, acuratețe și fiabilitate.

Creșterea eficienței și acurateței

Printre motivele convingătoare pentru instalarea unei rețele fără fir, trebuie luate în considerație beneficiile continue datorate productivității. Dacă beneficiile rezultate ca urmare a economiilor realizate acoperă costurile asociate cu instalarea și funcționarea unei rețele fără fir, o astfel de rețea este avantajoasă. Obținerea unui profit dintr-o investiție motivează cu siguranță pe oameni să aloce bani pentru sisteme noi.

Exemplu legat de activitatea de birou

Ca bază de creștere a productivității, trebuie luată în considerație achiziționarea de laptopuri echipate la standardul 802.11. Acestea permit angajaților să-și citească e-mail-urile, să răspundă la acestea și să acceseze Internetul în timpul ședințelor, presupunând că utilizatorii pot să participe la discuții atunci când este necesar, fiind simultan preocupați și de laptopuri. Chiar dacă acest lucru poate să pară banal, câștigul în productivitate poate fi important.

Dacă un utilizator participă la ședințe timp de 3 ore pe zi și își ocupă câte 15 minute din fiecare oră de ședință pentru a răspunde la e-mail-uri și pentru a efectua alte activități bazate pe Internet, acel utilizator dispune de 45 de minute în plus, în fiecare zi, pentru a îndeplini alte sarcini. Această socoteală pare a fi destul de rezonabilă, considerând-o ca medie pentru o persoană.

Câștigul de productivitate corespunzător celor 45 de minute rezultă din economia realizată de companie care depinde de cheltuielile pe unitatea de timp pentru angajatul respectiv. La un quantum de 50 \$ pe oră, economia este de 37,5 \$ pentru fiecare persoană, pe zi. O firmă mică, cu 20 de utilizatori, va economisi 750 \$ pe zi, 15 000 \$ pe lună, 180 000 \$ pe an și așa mai departe. Luând în considerație un cost de

40 000 \$ pentru hardware-ul unui LAN fără fir, rezultă că investiția se amortizează în mai puțin de trei luni! Chiar dacă se iau în considerație și costurile pentru achiziționarea de laptopuri noi pentru toți angajații, o firmă începe să obțină beneficii în mai puțin de un an, în cazul acestui exemplu simplu.

În afară de câștigul în productivitate, rețelele fără fir oferă și următoarele avantaje, în cazul muncii de birou:

- Utilizatorii pot continua să lucreze cu rețeaua atunci când compania efectuează modificări de amenajări interioare, lucru care se produce frecvent în corporații.
- Angajații vizitatori pot accesa cu ușurință serverele și aplicațiile companiei, prin intermediul rețelei, de oriunde din sediul firmei.
- Compania poate implementa și alte aplicații fără fir, pe baza rețelei existente, cum ar fi telefoanele mobile, economisind astfel bani.

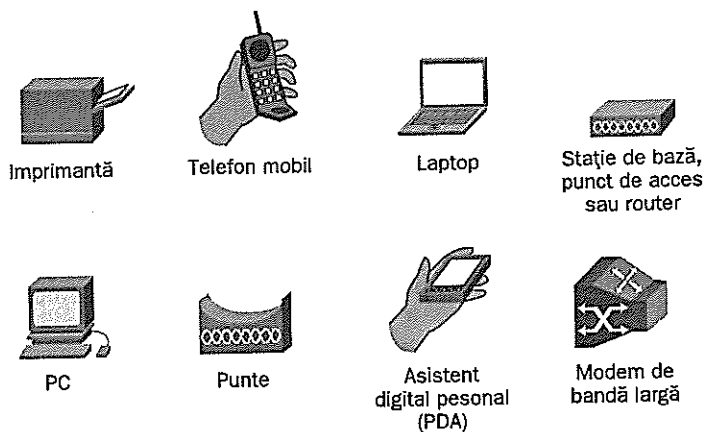
Exemplu legat de un depozit

Mobilitatea stă la baza realizării mai rapide a sarcinilor și cu mai puțini oameni. Imaginați-vă un transport de piese de schimb auto care ajunge la un centru de distribuție. Pe măsură ce camioanele sunt descărcate, sunt scanate codurile de bare de pe cutii, cu un colector de date manual, fără fir. Codul de bare conține un număr unic destinat identificării, care este transmis în mod automat, pe loc, către sistemul de administrare al depozitului pentru a indica recepționarea respectivei piese de schimb. Sistemul le indică, apoi, funcționarilor depozitului, prin intermediul ecranului colectorului de date, unde anume trebuie plasată cutia în depozit sau faptul că aceasta trebuie transportată direct la un anume client.

Dacă piesa respectivă rămâne în depozit, sistemul tipărește o etichetă care va fi lipită pe cutie, care identifică poziția de stocare stabilită, din depozit. Dacă piesa trebuie transportată la un client, sistemul va imprima ruta și informațiile de expediere pe o etichetă pe care un funcționar al depozitului o va lipi pe cutie. Cutia va putea fi apoi livrată la destinația corectă, fie că rămâne în depozit fie că este destinată unui camion pentru expedieri.

- **Titluri și subtitluri în limbaj netehnic** — În titlurile și subtitlurile folosite pe parcursul lucrării a fost, pe cât posibil, evitată utilizarea termenilor tehnici, în locul acestora fiind utilizate cuvinte care au conotații care subliniază anumite lucruri despre conceptele evidențiate.

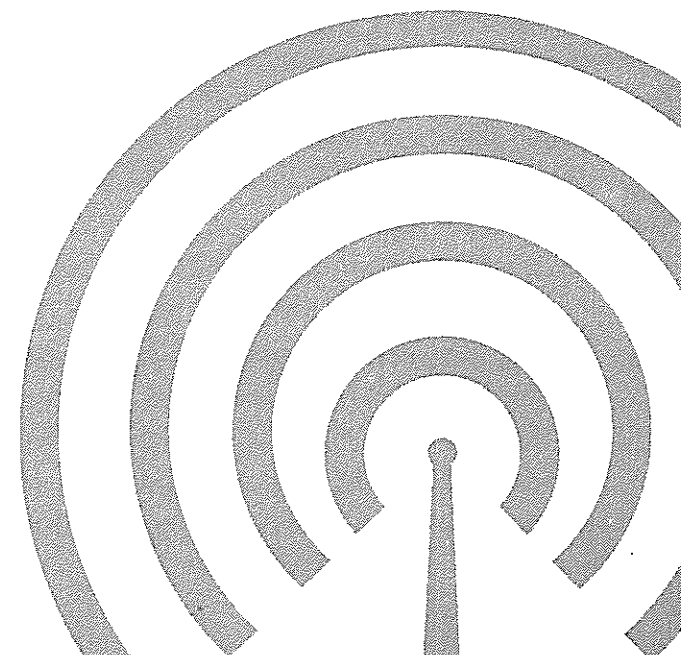
Pentru a reprezenta componentele de rețea și conexiunile, ilustrațiile din această carte utilizează următoarele pictograme:



Ce veți învăța

După citirea acestui capitol, veți putea:

- ✓ să faceți comparație între PAN-uri, LAN-uri, MAN-uri și WAN-uri fără fir;
- ✓ să recunoașteți exemplele generale de aplicații ale rețelelor fără fir;
- ✓ să înțelegeți avantajele rețelelor fără fir.





Utilizarea acestui sistem de recepționare permite companiei să reducă cantitatea de bunuri depozitată prin redirectionarea imediată a comenzilor primite către clienții respectivi. Totodată, sistemul elimină înregistrările pe hârtie și introducerea manuală a datelor. Însă, cel mai important lucru este acela că firma livrează comenzile clienților, mai rapid. În general, sistemul permite unei companii să realizeze câștiguri incredibile în eficiență și acuratețe prin comparație cu procesul pe bază de înregistrări pe hârtie, care produce adesea erori. Urmărirea pieselor pe baza înregistrărilor pe hârtie, urmată de introducerea manuală a datelor în sistemul de administrare al depozitului, prin intermediul unui terminal de birou, crește semnificativ probabilitatea de apariție a erorilor și necesită un personal numeros pentru a fi realizată.

Exemplu legat de un spital

Într-un spital, o rețea fără fir poate ajuta la salvarea de vieți omenești, prin îmbunătățirea vitezei și a preciziei livrării medicamentelor către pacienți. În conformitate cu normele guvernamentale, spitalele trebuie să realizeze o evidență exactă a narcoticelor, ceea ce îi determină pe administratori să impună metode de evidență strictă a cantităților de narcotice, adesea bazate pe înregistrări pe hârtie. Însă, utilizarea unei rețele fără fir permite folosirea unui scanner de mână pentru codurile de bare, ceea ce conduce la un proces de inventariere și de selectare a medicamentelor cu până la 300% mai rapid și mult mai exact.

În plus, o asistentă medicală poate verifica primirea medicației potrivite pentru un anume pacient scanând atât recipientul cu medicamentul, cât și brățara de identificare a pacientului. Acest lucru reduce semnificativ posibilitatea de a da un medicament altui pacient decât celui căruia îi era destinat. Mai mult, sistemul poate verifica dacă nu cumva pacientul este alergic la tipul de medicament pe care îl primește. Rețeaua fără fir face ca această aplicație să fie realizabilă într-un mediu spitalicesc extrem de mobil.

Multe alte aplicații conduc la suficiente câștiguri în eficiență și acuratețe ceea ce face ca instalarea unei rețele fără fir să merite să fie făcută. Obiectivul este cuantificarea atenției a beneficiilor și compararea acestora cu costurile sistemului.

Creșterea fiabilității

Cablurile sunt, în mod inerent, nefiabile, din cauza coroziunii și a întrebuințării nepotrivite. Instalarea improprie și distrugerea cablurilor sunt motivele principale din cauza cărora se defectează rețelele. De exemplu, un tehnician de la telefoane

poate să taie din neatenție un cablu de rețea, atunci când remediază o problemă apărută la sistemul telefonic. Acest lucru produce întreruperi în funcționarea rețelei, pe perioade de timp relativ lungi, până când administratorul de rețea remediază defectiunea.

Vremea rea, cum ar fi uraganele sau tornadele, poate afecta substanțial legăturile pe bază de fir dintre clădiri, atât aeriene cât și subterane. Acest tip de defecțiuni blochează, în mod frecvent, accesul la aplicații importante pentru utilizatorii dintr-o clădire întreagă. Chiar dacă, în general, rețelele cu cablu realizează performanțe superioare față de echivalenții lor fără fir, susceptibilitatea la întreruperi conduce la indisponibilități inacceptabile.

O rețea fără fir reduce în mod apreciabil problemele legate de distrugerile fizice. Disponibilitatea sistemelor crește, oferind utilizatorilor conectivitate în mare parte din timp. O rețea cu cablu poate fi necesară atunci când o rețea fără fir nu poate oferi performanțele cerute, însă, în acest caz, o rețea fără fir poate furniza o legătură de rezervă. Combinația dintre legăturile de comunicații cu fir și cele fără fir, realizate între clădiri, asigură un sistem fiabil, de înaltă performanță.

Rezumatul capitolului

O rețea fără fir elimină cablurile dintre dispozitivele de calcul (cum ar fi PDA-urile și laptopurile) și rețele existente. Acest lucru permite dispozitivelor de calcul și utilizatorilor acestora să fie extrem de mobili în timp ce accesează Internetul și aplicațiile de corporație. Oriunde s-ar afla cineva, într-un aeroport, acasă sau la serviciu, persoana respectivă poate să rămână conectată.

Diferitele tipuri de rețele fără fir oferă servicii pentru o varietate de aplicații acasă, la serviciu, în spitale și în spațiile publice, unde utilizatorii pot beneficia de accesul mobil la serviciile de rețea. Capacitatea de a asigura aplicații mobile complete este adesea suficientă pentru a justifica folosirea rețelelor fără fir. Totuși, în unele cazuri, o firmă trebuie să analizeze cu atenție câștigurile potențiale în eficiență, precizie și fiabilitate asigurate de o rețea fără fir pentru a vedea dacă costurile sistemului merită să fie suportate.

CAPITOLUL 1

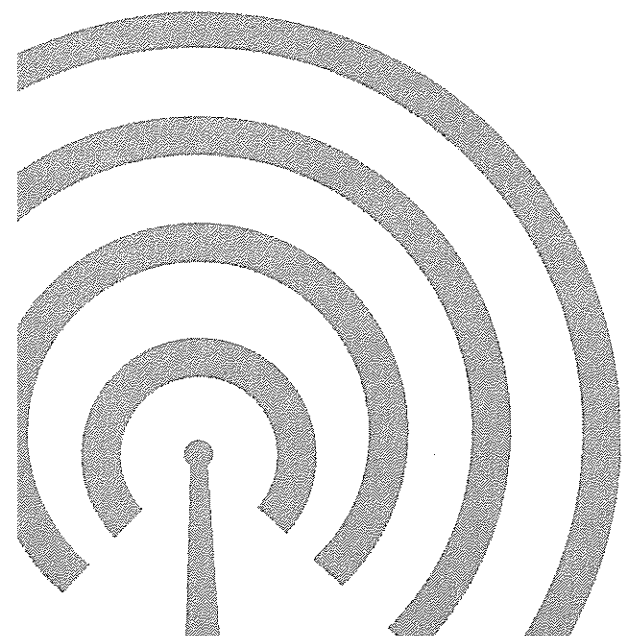
Lumea rețelelor fără fir: o introducere în concepte

Rețelele fără fir joacă un rol crucial în viața oamenilor, fie că aceștia se află la serviciu, acasă sau în spațiile publice. Chiar dacă o rețea fără fir are un scop simplu, acela de a realiza o legătură între utilizatori și sursele de informație, fără a fi utilizate cabluri, conceptele critice privitoare la rețelele fără fir trebuie să fie însușite înainte de a înțelege cum operează acestea. Acest capitol conține o definiție detaliată a tipurilor de rețele fără fir și prezintă avantajele pe care acestea le oferă utilizatorilor, în diferite aplicații.

Definirea tipurilor de rețele fără fir

O rețea fără fir asigură posibilitatea utilizatorilor de a comunica și de a accesa informațiile, fără folosirea cablurilor. Acest lucru oferă libertatea de mișcare și capacitatea de a extinde aplicațiile în diferite părți ale unei clădiri, ale unui oraș sau aproape oriunde în lume. De exemplu, cei care accesează Internetul de acasă pot face la fel dintr-un loc liniștit, departe de copiii gălăgioși, sau din fața televizorului, cu toată familia alături. Rețelele fără fir permit oamenilor să interacționeze prin intermediul e-mail-ului sau al navigării pe Internet, dintr-o locație preferată.

Rețele fără fir sunt utilizate de mulți ani. De fapt, formele incipiente ale comunicării fără fir includ și acoperirea și descoperirea focului cu pieile de bizon, de către indienii nord-americani, pentru a transmite, cu ajutorul fumului, semnale către semenii aflați la mari distanțe. De asemenea, folosirea pulsurilor de lumină pentru a transmite informații între nave, prin codul Morse, a fost și este încă o formă importantă de comunicare. Desigur că telefoanele mobile constituie și acestea o formă de comunicare fără fir foarte răspândită astăzi, prin care oamenii pot vorbi între ei când se află în diferite părți ale lumii.



Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. Care sunt atributele distinctive ale unei rețele fără fir prin comparație cu un sistem general de comunicații fără fir?
2. Care sunt tipurile de informații a căror transmisie poate fi asigurată de o rețea fără fir?
3. Care sunt cele patru tipuri de rețele fără fir?
4. Care este raza de acțiune maximă obișnuită a unei rețele PAN fără fir?
5. Adevărat sau fals: O rețea PAN fără fir consumă o putere scăzută de la micile dispozitive de calcul de mână.
6. Care sunt standardele uzuale pentru LAN-urile fără fir?
7. Care este standardul relativ nou care se aplică la MAN-urile fără fir?
8. Care este motivul pentru care WAN-urile fără fir nu satisfac, în mod efectiv, cerințele pentru rețelele fără fir, în interiorul clădirilor?
9. Care este aplicația uzuală a rețelelor fără fir în locuințe și în sediile de firme mici?
10. Care sunt exemplele de aplicații ale WAN-urilor fără fir?

Ce veți învăța

După citirea acestui capitol, veți putea:

- ✓ să înțelegeți care sunt componentele unei rețele fără fir;
- ✓ să descoperiți elementele generale ale arhitecturii rețelelor fără fir;
- ✓ să înțelegeți modul în care „curg” informațiile printr-o rețea fără fir.

Există multe tipuri de comunicații fără fir, însă atributul distinctiv al rețelei fără fir este acela că schimbul de informații se realizează între dispozitive de calcul. Aceste dispozitive includ: *asistenți digitali personali* (în limba engleză: *personal digital assistant* — acronim *PDA*), laptopuri, calculatoare personale (PC-uri), servere și imprimante. Dispozitivele de calcul posedă procesor, memorie și o modalitate de realizare a unei interfețe cu un anumit tip de rețea. Telefoanele mobile tradiționale nu corespund acestei definiții a dispozitivelor de calcul, însă, telefoanele mobile de generație mai nouă și chiar și echipamentele audio (cum sunt căștile fără fire) au început să încorporeze putere de calcul și adaptoare de rețea. În cele din urmă, majoritatea produselor electronice vor oferi posibilitatea de conectare la rețele fără fir.

Ca și în cazul rețelelor bazate pe cablu sau pe *fibră optică*, rețelele fără fir transportă informația între dispozitive de calcul. Informația se poate prezenta sub forma mesajelor e-mail, a paginilor Web, a înregistrărilor din bazele de date sau a fișierelor audio ori video. În cele mai multe cazuri, rețelele fără fir transferă *date*, cum ar fi mesajele e-mail sau fișierele, însă îmbunătățirea performanțelor acestora a condus la posibilitatea de a realiza și comunicații audio și video.

După cum vom vedea în capitolul 3, intitulat *Fundamentele semnalelor de radiofrecvență și ale semnalelor luminoase: mediul invizibil*, rețelele fără fir folosesc atât unde radio cât și unde infraroșii ca mediu de comunicare între utilizatori, servere și baze de date. Aceste mijloace de comunicare sunt invizibile pentru ochiul uman. În plus, mediul efectiv (aerul) este transparent pentru utilizator. Majoritatea producătorilor integrează acum plăci de rețea fără fir (NIC-uri, numite și adaptoare) și antene în dispozitivele de calcul fără ca acest lucru să fie vizibil pentru utilizator. Acest lucru face ca aceste dispozitive de calcul să fie mobile și ușor de utilizat.

Rețelele fără fir se împart în câteva categorii, în funcție de mărimea ariei fizice pe care o pot acoperi. Următoarele tipuri de rețele fără fir satisfac necesitățile diversilor utilizatori:

- rețea personală fără fir (în limba engleză: wireless personal-area network — acronim PAN).
- rețea locală fără fir (în limba engleză: wireless local-area network — acronim LAN).
- rețea metropolitană fără fir (în limba engleză: wireless metropolitan-area network — acronim MAN).
- rețea extinsă fără fir (în limba engleză: wireless wide-area network — acronim WAN).

Acești termeni sunt, pur și simplu, o extensie a numelor tipurilor principale de rețele pe bază de cabluri (cum sunt LAN-urile și WAN-urile) care erau utilizate cu ani buni înainte de apariția rețelelor fără fir.

Tabelul 1.1 prezintă o scurtă comparație între aceste forme de rețele fără fir. Fiecare tip de rețea are calități complementare care satisfac solicitări diferite. Secțiunile următoare descriu pe scurt fiecare tip de rețea fără fir.

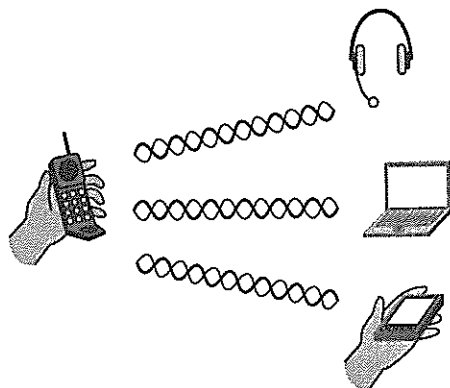
Tabelul 1.1 Comparație între tipurile de rețea fără fir

Tip	Arie de acoperire	Performanță	Standarde	Aplicații
PAN fără fir	încăpere	medie	Bluetooth, IEEE 802.15 și IrDA	înlocuirea cablurilor pentru periferice
LAN fără fir	clădire sau complex de clădiri	înaltă	IEEE 802.11, Wi-Fi și Hiper LAN	extensii mobile ale rețelelor cu cabluri
MAN fără fir	oraș	înaltă	brevet, IEEE 802.16 și WIMAX	rețele fără fir fixe, între domiciliu și sedii de companii și Internet
WAN fără fir	globală	scăzută	CDPD și Cellular 2G, 2.5G sau 3G	acces mobil la Internet din zone exterioare unor locații

PAN-uri fără fir

Așa cum se arată în figura 1.1, PAN-urile fără fir au o rază de acoperire relativ scurtă (până în 17 metri) și sunt cele mai eficiente pentru a satisface necesitățile de transmisie pentru o încăpere relativ mică sau o arie personală. Performanțele unei rețele PAN fără fir sunt medii, având o *viteză de transmisie a datelor* de până la 2 Mbps. Aceste caracteristici o recomandă pentru înlocuirea cablurilor în multe situații.

Figura 1.1. Rețeaua personală (PAN) fără fir permite interconectarea dispozitivelor de calcul din apropierea utilizatorului



De exemplu, o rețea PAN fără fir poate asigura sincronizarea unui PDA cu un laptop sau un PC. Tot așa, o rețea PAN fără fir poate asigura conectivitate fără cablu pentru o imprimantă. Avantajul eliminării încălcelii de cabluri, atunci când sunt utilizate periferice conectate astfel, este evident, iar instalarea inițială a perifericelor și mutarea acestora sunt ușor de realizat.

Consumul de energie electrică scăzut, ca și dimensiunile reduse ale majorității *transceiverelor*¹ pentru PAN-uri fără fir, fac posibilă dotarea efectivă cu asemenea componente a diverselor dispozitive de dimensiuni reduse echipate cu procesoare de calculatoare. Consumul redus permite dispozitivului de calcul să opereze perioade lungi de timp fără a consuma bateriile. Acest lucru conduce, desigur, la evitarea unor reîncărcări dese ale bateriilor de către utilizator.

De exemplu, consumul scăzut de energie a condus la implemetarea cu succes a PAN-urilor fără fir în telefoanele celulare, în PDA-uri și în dispozitive audio cu căști fără fir. Telefonul poate realiza o legătură permanentă cu agenda de adrese din PDA, astfel încât toate numerele de telefon de acolo să fie disponibile atunci când se realizează convorbiri telefonice. Utilizatorul poate folosi un set de căști fără fir pentru a vorbi la telefon sau pentru a asculta muzica stocată în format digital pe PDA. Acest lucru evită agățarea firelor de diferite lucruri atunci când lucrați sau ascultați muzică.

¹ Emițătoare-receptoare. Dispozitive care transmit și recepționează semnale analogice sau digitale (n.tr).

În plus, unele PAN-uri fără fir pot interconecta laptopuri și PC-uri în scopul partajării de conexiuni Internet și de aplicații. Acest lucru se poate realiza pentru rețele limitate la o încăpere. O mai bună conectivitate fără fir pentru o clădire, o asigură LAN-urile fără fir.

Cele mai multe PAN-uri fără fir folosesc undele radio pentru a transporta informația prin aer. De exemplu, specificațiile *Bluetooth* definesc operarea PAN-urilor fără fir în banda de frecvență 2,4 MHz cu raza de acțiune de 17 metri și o viteză de transmisie de până la 2Mbps. În plus, standardul IEEE (Institute of Electrical and Electronic Engineers) *802.15* încorporează specificația Bluetooth pentru PAN-uri fără fir. Aceste tehnici oferă o soluție fiabilă, pe termen lung, pentru conectarea dispozitivelor de calcul pe o arie restrânsă.

Unele PAN-uri fără fir utilizează lumină infraroșie pentru transportul informației de la un punct la altul. Specificațiile Infrared Data Association (IrDA) definesc utilizarea razelor infraroșii directe care oferă o distanță de acțiune de până la un metru și o viteză de transmisie de până la 4 Mbps. Avantajul utilizării luminii infraroșii este acela că nu se produc interferențe cu frecvențele radio, însă cerințele de plasare în raza de vedere a dispozitivelor de calcul (fără obstacole între acestea) limitează poziționarea componentelor fără fir. De exemplu, compartimentarea unei încăperi blochează calea semnalelor de lumină infraroșie, ceea ce reduce raza de utilizare a dispozitivelor fără fir.



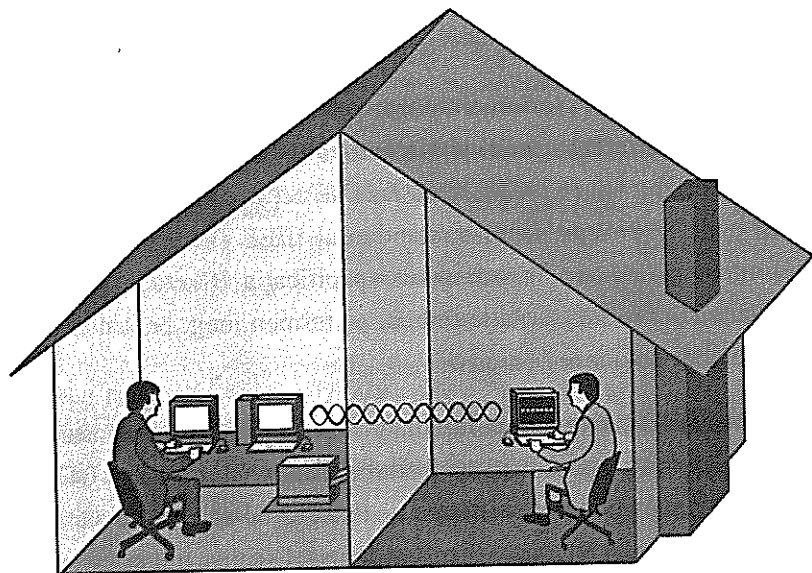
Notă

În capitolul 4, intitulat *PAN-uri fără fir: rețele pentru spații restrânse*, veți găsi detalii privitoare la tehnicile și produsele PAN.

LAN-uri fără fir

LAN-urile fără fir asigură performanțe înalte în arii din preajma unor clădiri de birouri, fabrici sau locuințe (vezi figura 1.2). Utilizatorii din aceste arii posedă, de regulă, laptopuri, PC-uri și PDA-uri cu ecrane mari și procesoare puternice care oferă posibilitatea utilizării de aplicații de nivel înalt de către utilizatorii finali. LAN-urile fără fir satisfac în mod eficient nevoile de conectivitate pentru aceste tipuri de dispozitive de calcul.

Figura 1.2. Rețeaua locală (LAN) fără fir oferă posibilitatea interconectării dispozitivelor de calcul aflate în interiorul unei clădiri



O firmă, de exemplu, poate instala o rețea LAN fără fir pentru a oferi posibilitatea accesului mobil la aplicațiile de corporație de pe laptopuri. În cazul unui astfel de tip de sistem, un utilizator poate folosi servicii de rețea din sala de conferințe sau din alte locuri aflate la distanță de propriul birou. Acest lucru permite o muncă mai eficientă a angajaților care pot lucra la distanță de birourile proprii și pot, astfel, colabora între ei.

LAN-urile fără fir asigură cu ușurință niveluri de performanță care permit aplicațiilor de nivel înalt să ruleze fără piedici. De exemplu, utilizatorii unei rețele LAN fără fir pot vizualiza cu ușurință un fișier mare atașat la un mesaj e-mail sau o secvență video de pe un server. Asigurând viteze de transmisie de până la 54 Mbps, o rețea LAN fără fir poate satisface aproape toate cerințele oricărei aplicații de rețea folosită acasă sau la serviciu.

LAN-urile fără fir sunt similare LAN-urilor *Ethernet* tradiționale, cu cabluri, în ceea ce privește performanțele, componentele, costurile și operarea.

Datorită implementării pe scară largă a adaptoarelor LAN fără fir în laptopuri, majoritatea furnizorilor de rețele fără fir publice realizează LAN-uri fără fir pentru a oferi servicii mobile de bandă largă pentru accesul la Internet. Utilizatorii din raza unei rețele LAN fără fir publice a unui spațiu aglomerat (punct fierbinte) cum ar fi un hotel sau un aeroport, pot accesa poșta electronică sau pot naviga pe Internet contra unei taxe (dacă nu cumva serviciul este oferit gratuit). Dezvoltarea rapidă a LAN-urilor fără fir publice a făcut ca Internetul să devină disponibil pentru persoane aflate în arii în care oamenii tind să se strângă la un loc.

IEEE 802.11 este cel mai răspândit standard pentru LAN-uri fără fir, cu versiuni care operează pe benzile de frecvență de 2,4 GHz și 5 GHz. O problemă a standardului 802.11 este interoperabilitatea limitată între diferitele versiuni ale acestuia. De exemplu, un dispozitiv de calcul LAN fără fir care utilizează un adaptor 802.11a nu poate fi conectat cu un alt dispozitiv de calcul care implementează versiunea 802.11b. În plus, există și alte probleme legate de standardul 802.11, cum ar fi securitatea limitată a transmisiei datelor, aspect discutat în capitolele următoare ale acestei cărți.

Pentru a rezolva problemele legate de standardul 802.11, Wi-Fi Alliance a încorporat anumite funcții ale standardului 802.11 într-un standard la care aceștia se referă sub numele de *Wireless Fidelity (Wi-Fi)*. Dacă un produs LAN fără fir se conformează standardului Wi-Fi, acesta are asigurată interoperabilitatea cu alte produse Wi-Fi. Deschiderea suplimentară oferită de Wi-Fi asigură posibilitatea operării unor utilizatori diverși pe aceeași LAN fără fir. Acesta este un aspect foarte important pentru LAN-urile fără fir publice.

Notă



În capitolul 5, intitulat *LAN-uri fără fir: rețele pentru clădiri și complexe de clădiri*, veți găsi detalii privitoare la tehnicile și produsele LAN fără fir.

MAN-uri fără fir

MAN-urile fără fir acoperă arii de dimensiunile unui oraș mare. În cele mai multe cazuri, aplicațiile implică conectivitate fixă, dar anumite implementări asigură mobilitatea. De exemplu, un spital poate instala o rețea MAN fără fir pentru a asigura comunicațiile de date între sediul central și o clinică aflată la distanță. Similar, o companie

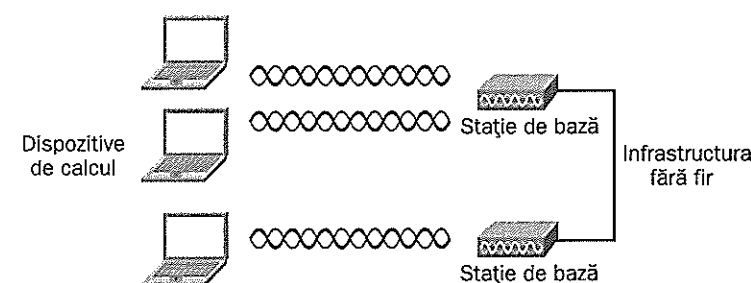
Arhitectura sistemului fără fir: cum funcționează rețelele fără fir

Rețelele fără fir utilizează componente similare cu cele folosite în rețelele cu fir; însă, rețelele fără fir trebuie să convertească semnalele purtătoare de informație într-o formă potrivită pentru transmisia prin mediul aerian. Chiar dacă rețelele fără fir contribuie direct numai pe o porțiune din întreaga infrastructură a rețelei, este necesar să se acorde atenție tuturor funcțiilor rețelei pentru a contracara problemele cauzate de mediul fără fir. Acest capitol discută conceptele comune tuturor tipurilor de rețele fără fir, punând accentul pe componentele de rețea și pe semnalele purtătoare de informație.

Componentele sistemului rețelei fără fir

O rețea fără fir constă în câteva componente care asigură comunicațiile, folosind undele radio sau undele de lumină care se propagă prin mediul aerian. Câteva dintre aceste componente se suprapun cu cele ale rețelelor cu fir, însă o atenție deosebită se cere acordată tuturor componentelor atunci când se instalează o rețea fără fir. Figura 2.1 prezintă aceste componente primare.

Figura 2.1. Rețelele fără fir includ dispozitive de calcul, stații de bază și infrastructura fără fir



Utilizatori

Un utilizator poate fi orice persoană sau dispozitiv care folosește, în mod direct, o rețea fără fir. Unul dintre cele mai comune tipuri de utilizatori sunt persoanele. De exemplu, o persoană care călătorește pentru afaceri și care accesează Internetul printr-o LAN fără fir publică dintr-un aeroport, este un utilizator. În unele cazuri, însă, utilizatorul poate să nu fie uman. De exemplu, un robot poate recepționa instrucțiunile, prin intermediul unei rețele fără fir, de la un calculator central care controlează un proces de fabricație. Pentru că rețeaua fără fir există pentru a-i servi utilizatorului, utilizatorul este componenta care beneficiază de serviciile oferite de aceasta. Ca urmare, utilizatorii sunt o parte importantă a rețelei fără fir.

Utilizatorii inițiază și finalizează utilizarea unei rețele fără fir, ceea ce face ca termenul de utilizator final să fie adecvat. De regulă, un utilizator operează pe un *dispozitiv de calcul*, care adesea realizează o varietate de funcții de tip aplicații specifice, pe lângă faptul că oferă o interfață cu rețeaua fără fir.

Utilizatorii rețelelor fără fir tind să fie mobili, mișcându-se în permanență prin clădire, campus sau oraș. Mobilitatea este unul dintre cele mai evidente avantaje ale unei rețele fără fir. De exemplu, o persoană care se plimbă printr-un centru de conferințe în timp ce trimite și primește e-mail-uri prin intermediul unui PDA, uzează de mobilitate. În acest caz, PDA-ul trebuie să realizeze o conexiune continuă sau frecventă la infrastructura unei rețele fără fir.

Unii utilizatori pot să solicite doar portabilitatea; adică, ei stau într-o anumită locație în timp ce utilizează rețeaua fără fir pentru o anumită perioadă de timp. Un exemplu al acestui tip de utilizare este cineva care operează pe un laptop conectat fără fir dintr-o sală de conferințe. Utilizatorul pornește laptopul după ce se așază în sala de conferințe și îl oprește înainte de a o părăsi. Prin urmare, nu este nevoie ca rețeaua fără fir să permită mișcarea continuă a utilizatorului.

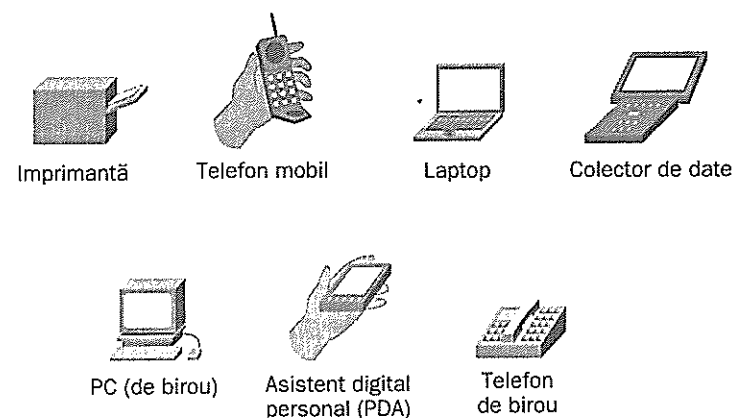
Alți utilizatori pot fi efectiv staționari, adică ei operează dintr-un anumit loc o perioadă de timp nedefinită. Un exemplu al unui astfel de tip de utilizator este o persoană care lucrează într-un birou pe un calculator conectat fără fir. Cea mai mare deosebire dintre un utilizator staționar și unul portabil constă în aceea că utilizatorul staționar nu solicită nici o formă de funcții de roaming¹. În anumite situații, funcțiile de roaming sunt dificil de implementat.

¹ Funcțiuni care permit operarea unui utilizator care își poate schimba locația — de la verbul din limba engleză *to roam* = a cutreiera, a hoinări (n. tr.).

Dispozitive de calcul

Există multe tipuri de dispozitive de calcul, numite uneori și clienți, care operează într-o rețea fără fir. Unele dispozitive de calcul pot fi proiectate, în mod specific, pentru utilizatori, în timp ce unele sunt sisteme finale. În general, fiecare dispozitiv de calcul poate comunica cu oricare altul aflat în aceeași rețea fără fir. Figura 2.2 prezintă o serie de dispozitive de calcul pentru rețelele fără fir.

Figura 2.2. Dispozitive de calcul pentru rețelele fără fir dedicate pentru aplicații diverse



Pentru a asigura aplicații mobile, adesea, dispozitivele de calcul sunt mici, ceea ce le face ușor de purtat în permanență de către oameni. În general, aceste dispozitive au ecrane și tastaturi de dimensiuni limitate și baterii mici. Dispozitivele sunt mobile, dar nu pot asigura decât anumite aplicații.

Însă, pentru aplicații portabile sau staționare, dispozitivele de calcul sunt mult mai mari. Aceste dispozitive au, în general, ecrane și tastaturi mai mari, ceea ce le face mai potrivite pentru a fi utilizate la navigarea pe Internet și în alte aplicații care cer performanțe relativ ridicate. Însă, problema cu aceste dispozitive este că au o greutate mai mare și sunt dificil de purtat dintr-un loc în altul.

Dispozitivele de calcul dintr-o rețea fără fir includ și sisteme finale cum sunt serverele, bazele de date și site-urile Web. De exemplu, site-ul Web <http://www.cnn.com> include știri pe care cineva le poate vizualiza, printr-o conexiune

asigurată de o LAN fără fir publică, dintr-o cameră de hotel. În mod similar, un funcționar poate să se conecteze la un sistem de administrare a unui depozit, care se comportă ca un dispozitiv de calcul de tip sistem final.

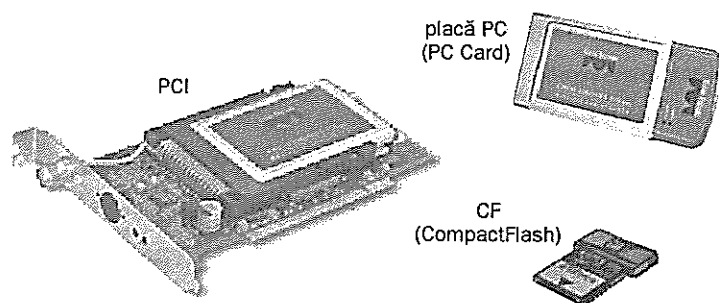
Utilizatorii pot adapta multe dispozitive de calcul existente pentru a putea opera într-o rețea fără fir. De exemplu, un utilizator poate cumpăra și instala o placă interfață de rețea fără fir (NIC) pentru ca laptopul său să poată opera într-un anumit tip de rețea fără fir. Unele dispozitive, cum sunt scanerele fără fir pentru coduri de bare, operează numai în rețele fără fir.

De asemenea, un dispozitiv de calcul posedă un sistem de operare, cum ar fi Windows XP, LINUX sau MAC OS. Sistemul de operare rulează software-ul necesar pentru realizarea aplicațiilor fără fir. În anumite cazuri, sistemul de operare are incluse caracteristici care îmbunătățesc operarea în rețele fără fir. De exemplu, Windows XP posedă capacitatea de a identifica, în mod automat, LAN-urile fără fir și de a se conecta la acestea.

Plăci interfață de rețea (plăci de rețea – NIC-uri)

Placa interfață de rețea (în limba engleză: *network interface card* – acronim *NIC*) furnizează interfața dintre dispozitivul de calcul și infrastructura rețelei fără fir. Placa se montează în interiorul dispozitivului de calcul, însă sunt disponibile și adaptoare de rețea externe care se montează în exteriorul dispozitivului de calcul. Figura 2.3 prezintă exemple de câteva tipuri de NIC-uri fără fir.

Figura 2.3. NIC-urile fără fir au diferite tipuri de factori de formă



Standardele pentru rețele fără fir definesc modul de operare al NIC-urilor fără fir. De exemplu, o NIC LAN fără fir poate implementa standardul IEEE 802.11b. În acest caz, placa de rețea fără fir va putea să constituie o interfață numai cu o infrastructură de rețea fără fir care se conformează standardului 802.11b. Prin urmare, utilizatorii trebuie să se asigure că NIC-urile fără fir pe care le aleg sunt potrivite pentru tipul de infrastructură de rețea fără fir la care doresc să se conecteze.

De asemenea, NIC-urile se conformează anumitor factori de formă, care definesc magistrala fizică și electrică a interfeței, care permite plăcii să comunice cu dispozitivele de calcul. Din nou, utilizatorul trebuie să se asigure că NIC-ul fără fir ales se va potrivi cu dispozitivul de calcul. În continuare, sunt enumerați factorii de formă disponibili pentru NIC-uri interne ale rețelelor fără fir:

- **Industry-Standard Architecture (ISA)** — ISA există de la începutul anilor 1980. Din această cauză, magistralele ISA sunt foarte răspândite. În ciuda performanțelor limitate, aproape toate PC-urile fabricate până de curând aveau cel puțin o magistrală ISA. Totuși, magistralele ISA au fost abandonate pentru a se ține pasul cu evoluția din lumea calculatoarelor, iar astăzi sunt disponibile alternative cu viteze de transfer mai mari. ISA nu influențează foarte mult performanțele LAN-urilor fără fir 802.11b. Oricum, nu este recomandabil să achiziționați plăci ISA noi, pentru că există posibilitatea ca acestea să devină depășite.
- **Peripheral Component Interconnect (PCI)** — Magistrala PCI este cea mai comună magistrală utilizată astăzi în PC-uri și are performanțe ridicate. Inițial, Intel a realizat și a lansat, în 1993, magistrala PCI, iar aceasta satisface necesitățile generațiilor recente de PC-uri pentru multimedia și grafică. Plăcile PCI au fost primele care au popularizat tehnicile „plug-and-play”, care permit o instalare ușoară a NIC-urilor. Circuitele PCI pot recunoaște plăcile PCI compatibile și pot lucra cu sistemul de operare al calculatorului pentru a stabili configurațiile pentru fiecare placă. Acest lucru economisește timp și previne bătaia de cap în cazul unui utilizator fără cunoștințe tehnice.
- **placa PC** (din limba engleză **PC Card**) — Placa PC a fost dezvoltată la începutul anilor 1990 de către Personal Computer Memory Card International Association (PCMCIA — Asociația Internațională pentru Plăci de Memorie pentru Calculatoare Personale). *Placa PC* este un dispozitiv de dimensiunile unei cărți de credit care oferă memorie extinsă, modemuri, conectivitate pentru dispozitive externe și capacitate de conectare la LAN-uri fără fir pentru dispozitive de calcul de dimensiuni

reduse, cum ar fi laptopurile și PDA-urile. De fapt, sunt cele mai larg răspândite NIC-uri disponibile azi. Au devenit mai populare decât ISA sau PCI datorită utilizării, în număr din ce în ce mai mare, a laptopurilor și a PDA-urilor.

Există posibilitatea utilizării unei plăci PC pe un PC de birou folosind un adaptor care convertește o placă PC în una PCI. Acest lucru permite cumpărarea unei singure plăci de rețea pentru a fi folosită pe ambele tipuri de calculatoare. Puteți lua placa PC cu dumneavoastră, într-o călătorie de afaceri — sau pentru a lucra acasă — și puteți să utilizați aceeași placă atunci când vă întoarceți la birou, pentru PC-ul pe care-l aveți acolo. Unele PDA-uri au nevoie de un dispozitiv sanie pentru a putea găzdui o placă PC montată sub PDA. Aceasta este singura cale de dotare cu capacitatea de conectare la rețelele fără fir pentru unele modele mai vechi de PDA-uri. Însă, combinația sanie, placă PC și PDA crește mult volumul și greutatea ansamblului limitând astfel posibilitățile de utilizare.

▪ **Mini-PCI** — O placă mini-PCI este o versiune de dimensiune mai mică a plăcii PCI standard pentru PC-uri, care se potrivește la dispozitivele de calcul mobile, mai mici. Are aceleași caracteristici și funcționalități ca și o placă PCI normală, însă dimensiunile sunt cam la un sfert din aceasta. Plăcile mini-PCI sunt integrate în laptopuri ca o opțiune pentru cumpărător. Un avantaj important al acestui tip de NIC radio este acela că eliberează slotul plăcii PC, care poate fi, în felul acesta, utilizat de alte dispozitive, cum ar fi extensiile de memorie și acceleratoarele grafice. În plus, fabricanții pot furniza NIC-uri fără fir tip mini-PCI la prețuri mai mici. Însă plăcile mini-PCI au și dezavantaje. Înlocuirea unei plăci mini-PCI necesită, de regulă, dezasambarea laptopului, ceea ce poate duce la anularea garanției producătorului. De asemenea, plăcile mini-PCI pot conduce la performanțe mai scăzute datorită faptului că acestea solicită calculatorului să execute o parte din procesare, dacă nu cumva toată procesarea necesară. În ciuda acestor neajunsuri, plăcile mini-PCI au devenit o tehnică solidă în lumea laptopurilor cu conectare fără fir.

▪ **CompactFlash** — SanDisk Corporation a produs pentru prima dată cardul *CompactFlash* (CF) în 1994, dar NIC-uri fără fir cu factori de formă CF nu au fost disponibile până de curând. Un card CF este mic, cântărind cam 15 grame și având o grosime de mai puțin de jumătate din grosimea unei plăci PC. Totodată, ocupă cam un sfert din volumul unei plăci PC radio. Cardurile CF consumă puțină energie, ceea ce permite ca bateriile să dureze mai mult decât în cazul dispozitivelor care folosesc plăci PC. Unele PDA-uri sunt produse direct cu interfețe CF, ceea ce face ca acestea să fie niște PDA-uri fără fir, ușoare și compacte. Dacă dispozitivul

de calcul nu posedă un slot CF, puteți achiziționa un adaptor astfel încât cardul CF să se potrivească într-un slot de placă PC standard. Un card CF este calea de urmat, mai ales pentru dispozitivele de calcul compacte.

În afară de NIC-urile interne, există o varietate de interfețe de rețea externe care se conectează la dispozitivele de calcul prin porturi seriale, paralele sau USB. Acestea pot fi considerate ca fiind adecvate pentru calculatoare staționare, însă constituie o piedică în calea mobilității pentru cele mai multe aplicații fără fir.

Așa cum este descris în detaliu în capitolul 3, intitulat *Fundamentele semnalelor de radiofrecvență și ale semnalelor luminoase: mediul invizibil*, o placă NIC fără fir include o antenă care convertește semnalele electrice în unde radio sau în unde de lumină care se propagă prin mediul aerian. Antenele utilizează multe tipuri de structuri care pot fi externe, interne, permanente sau detașabile. De exemplu, antena unei plăci PC, este, în general, atașată la capătul plăcii și iese în afara laptopului.

Plăcile mini-PCI, însă, pot avea o antenă aflată în interiorul marginii exterioare a monitorului laptopului. Unele NIC-uri au antene permanente, care realizează un anumit model de propagare a undelor. Alte NIC-uri permit înlocuirea antenei, ceea ce crește flexibilitatea în alegerea unei antene care satisface cel mai bine cerințele.

Mediul aerian

Aerul servește mai multor scopuri, cum ar fi: furnizarea mediului necesar pentru transmisia vocii, oferirea posibilității de realizare a transportului aerian și susținerea vieții. Totodată, aerul oferă mediul necesar pentru propagarea semnalelor de comunicații fără fir, care sunt inima unei rețele fără fir. Aerul este canalul prin care se transferă informația între dispozitivele de calcul și infrastructura fără fir. Gândiți-vă la comunicarea prin intermediul unei rețele fără fir ca fiind similară cu a vorbi cu cineva. Cu cât vă îndepărtați mai mult, cu atât este mai dificil să vă auziți unul pe celălalt, mai ales atunci când este prezent și un zgomot puternic.

Semnalele informațiilor transmise fără fir călătoresc tot prin aer, însă acestea au proprietăți speciale care permit propagarea pe distanțe relativ mari. Semnalele informațiilor transmise fără fir nu pot fi auzite de oameni, de aceea este posibil să fie amplificate la un nivel mai înalt fără să deranjeze urechea umană. Calitatea transmisiei depinde, însă, de obstacolele din aer care pot reduce puterea semnalelor, iar de aici rezultă și raza de acțiune, sau, dimpotrivă, le pot dispersa.

Ploaia, ninsoarea, smogul și fumul sunt exemple de fenomene care afectează propagarea semnalelor comunicațiilor fără fir. De fapt, o ploaie torențială serioasă poate limita raza de propagare a semnalelor cu 50%. Alte obstacole, cum ar fi copacii sau clădirile, pot influența propagarea semnalelor și performanța unei rețele fără fir. Aceste aspecte devin foarte importante atunci când se planifică instalarea unei MAN sau a unei WAN fără fir.

În cazul rețelelor fără fir, mediul aerian asigură propagarea undelor radio sau a celor luminoase care călătoresc de la un punct la altul. Aceste tipuri de semnale au fost folosite de mai bine de 100 de ani, însă ele rămân oarecum misterioase și nu foarte bine înțelese de majoritatea profesioniștilor calculatoarelor. Capitolul 3 oferă detalii despre caracteristicile semnalelor și despre atenuarea acestora, privite din perspectiva utilizării mediului aerian.

Infrastructuri de rețele fără fir

Infrastructura unei rețele fără fir interconectează utilizatorii și sistemele finale. Infrastructura poate fi formată din *stații de bază*, controlere de acces, software pentru conectivitatea aplicațiilor și dintr-un sistem de distribuție. Aceste componente asigură comunicațiile fără fir și îndeplinesc funcții importante necesare pentru diferite aplicații.

Stații de bază

Stația de bază este o componentă de infrastructură comună, care asigură o interfață între semnalele comunicațiilor fără fir care călătoresc prin mediul aerian și o rețea cu fir — numită adesea sistem de distribuție. Astfel, o stație de bază permite utilizatorilor să acceseze o paletă largă de servicii de rețea, cum ar fi navigarea pe Web, e-mail sau aplicațiile de baze de date. Stația de bază posedă, de obicei, un NIC fără fir care implementează aceeași tehnică de operare ca și NIC-ul fără fir al utilizatorului.

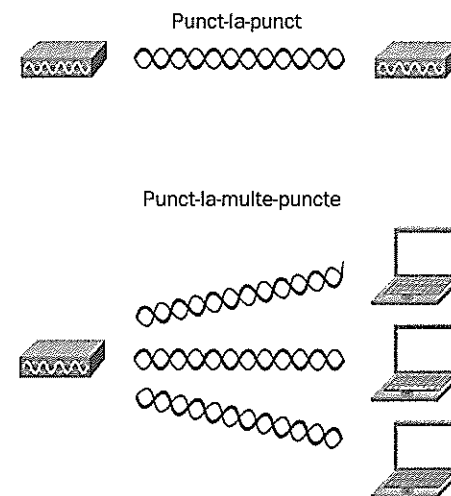
Stațiile de bază pot purta multe nume diferite, în funcție de scopul acestora. Un *punct de acces*, de exemplu, reprezintă generic o stație de bază pentru o rețea LAN fără fir. De exemplu, o serie de puncte de acces dintr-o rețea LAN fără fir asigură roaming-ul pe întreg cuprinsul unei clădiri/locație. NIC-ul din dispozitivul de calcul

al utilizatorului se conectează la cel mai apropiat punct de acces, oferind astfel o interfață cu sistemele din infrastructură și cu utilizatorii conectați la alte puncte de acces. Atunci când utilizatorul se mută în altă parte a clădirii/locației, care este mai apropiată de un alt punct de acces, NIC-ul acestuia se reconectează, în mod automat, la acest punct de acces pentru a menține o comunicație sigură, de calitate.

Porțile și routerele de rezidență sunt forme mai evoluate de stații de bază care asigură funcții suplimentare de rețea. Porțile pot avea funcții, cum ar fi controlul accesului și conectivitatea aplicațiilor, care le recomandă mai curând pentru rețelele publice, distribuite. Pe de altă parte, un *router* va putea asigura operarea mai multor calculatoare printr-o singură conexiune cu bandă largă.

Așa cum se arată în figura 2.4, o stație de bază poate asigura comunicații punct-la-punct sau comunicații punct-la-multe-puncte. Sistemele punct-la-punct permit semnalelor de comunicație să treacă de la o anumită stație de bază, sau de la un anumit dispozitiv de calcul, direct la o alta. Acesta este tipul de infrastructură comun, folosit pentru asigurarea legăturilor de comunicații fără fir la mare distanță. De exemplu, un *furnizor de servicii Internet fără fir* (în limba engleză: *wireless Internet service provider* — acronim *WISP*) poate utiliza acest sistem pentru a transporta semnalele de comunicații de la o stație de bază aflată la o locație îndepărtată — cum ar fi o locuință sau un sediu de firmă — la o stație de bază aflată lângă un centru de comunicații.

Figura 2.4. Stațiile de bază permit realizarea de configurații diverse



Așa cum rezultă și din nume, funcționalitatea punct-la-multe-puncte permite unei stații de bază să comunice cu mai multe dispozitive de calcul fără fir sau stații de bază. Un punct de acces dintr-o rețea LAN fără fir implementează o astfel de formă de comunicații. Punctul de acces reprezintă punctul unic în care sunt conectate mai multe dispozitive de calcul pentru a putea comunica între ele prin intermediul infrastructurii fără fir.

Controlere de acces

În absența unei protecții adecvate, a unui sistem de asigurare al calității serviciilor (în limba engleză: quality of service — acronim QoS) și a unor mecanisme de roaming în cadrul standardelor rețelei fără fir, companiile oferă soluții de control al accesului pentru a întări sistemele fără fir. Componenta cheie a acestor soluții este un controler de acces, care este, în mod tipic, un hardware aflat în porțiunea cu fir a rețelei dintre punctele de acces și partea protejată a rețelei. Controlerele de acces asigură „inteligenta” localizată în spatele punctului de acces, care controlează traficul dintre partea deschisă a rețelei fără fir și resursele importante ale acesteia. În unele cazuri, punctele de acces realizează și funcția de control al accesului.

Controlerele de acces sunt folosite la o gamă largă de aplicații. De exemplu, într-o rețea LAN fără fir publică, un controler de acces reglementează accesul la Internet prin autentificarea și autorizarea utilizatorilor, bazată pe o listă de abonați. În mod similar, o firmă poate implementa un controler de acces pentru a împiedica accesul unui hacker, aflat în parcare a companiei, la date și aplicații sensibile.

Utilizarea unui controler de acces reduce necesarul de puncte de acces „inteligente”, care sunt relativ scumpe și includ multe caracteristici care nu țin de standardele 802.11. În general, producătorii se referă la aceste puncte de acces mai inteligente ca fiind componente din categoria celor pentru întreprinderi. Partizanii controlerelor de acces, însă, argumentează că punctele de acces 802.11 ar trebui să se concentreze asupra calității semnalelor radio și asupra costurilor scăzute. De asemenea, partizanii controlerelor susțin că punctele de acces ar trebui să centralizeze funcțiile de control al accesului într-un controler de acces care să servească toate punctele de acces. Aceste puncte de acces „slabe” trebuie să implementeze, în primul rând, standardele de bază pentru rețelele fără fir (cum este IEEE 802.11) și nimic mai mult.

Utilizatorii controlerelor de acces evidențiază următoarele avantaje ale folosirii punctelor de acces slabe:

- **Costuri reduse** — Punctele de acces cu funcționalități limitate costă mai puțin, ceea ce conduce, în general, la costuri mai mici ale întregului sistem. Lucru acesta este adevărat, în mod special, pentru rețelele care necesită un număr mare de puncte de acces, cum ar fi un sistem de întreprindere. Utilizarea

punctelor de acces slabe conduce la economii de aproximativ 400 \$ pe punct de acces. În rețelele mai mari, valoarea acestor economii depășește cu mult costurile suplimentare legate de instalarea unui controler de acces, care se ridică la o medie de 5 000 \$.

- **Conectivitate deschisă** — Punctele de acces inteligente oferă îmbunătățiri ale securității și ale performanței pentru conectivitatea fără fir de bază pe care o realizează standardele rețelelor fără fir. Problema constă în faptul că, în multe situații, aceste îmbunătățiri sunt realizabile numai dacă dispozitivul utilizatorului implementează o NIC fără fir produsă de același fabricant care a realizat și punctul de acces. Acest lucru reduce semnificativ caracterul deschis al sistemelor și presupune limitări în alegerea producătorilor. Pe de altă parte, punctele de acces slabe pot comunica cu ușurință, folosind un *protocol* de rețea fără fir de bază, NIC-urile putând fi fabricate de mai mulți producători, în timp ce controlerul de acces asigură, în mod transparent, îmbunătățirile.
- **Întreținerea centralizată** — Un avantaj al plasării „inteligentei” rețelei într-un controler de acces constă în aceea că sistemul este mai ușor de întreținut, în primul rând pentru că există mai puține puncte în rețea la care trebuie intervenit. Dacă toată „inteligenta” rețelei se află în punctele de acces, personalul de întreținere trebuie să intervină în multe puncte atunci când configurează, monitorizează și depanează rețeaua. Un controler de acces permite ca punctele de acces să aibă mai puține funcții, limitându-se astfel necesitatea de a se interveni asupra acestor componente atunci când se realizează lucrările de întreținere.

Adesea, controlerele de acces asigură un control al accesului bazat pe porturi, ceea ce permite administratorilor de rețea să configureze accesul la anumite aplicații în funcție de utilizator. Portul, care este de fapt un număr (cum este 80 pentru http), corespunde unui anume tip de aplicație. De exemplu, un controler de acces poate bloca accesul la portul 80, ceea ce îl va forța pe utilizator să se conecteze² înainte de a putea să vizualizeze paginile Web. După ce utilizatorii introduc numele lor de utilizatori și parolele corespunzătoare, controlerul de acces le va valida identitățile prin intermediul unui server de autentificare. Aplicația de rețea poate să folosească, ca o alternativă, *certIFICATELE digitale* în scopul autentificării. Această funcție controlează accesul utilizatorului la rețeaua protejată.

² În limba engleză, *log on* și nu *connect*; ambele verbe se traduc prin *a conecta* deși se referă la procese diferite: primul se referă la procesul de inițiere a autentificării prin introducerea numelui de utilizator și a parolei, al doilea se referă la stabilirea conexiunii operaționale care permite utilizarea aplicației (n.tr.).

În general, controlerile de acces se ocupă de următoarele aspecte:

- **Autentificare** — Majoritatea controlerelor de acces posedă o bază de date încorporată pentru autentificarea utilizatorilor; unele însă, oferă interfețe externe pentru serverele de autentificare, cum ar fi *Remote Authentication Dial-In User Service (RADIUS)* sau *Lightweight Directory Access Protocol (LDAP)*. Pentru rețelele private, mai mici, o bază de date internă poate fi suficientă. Pentru rețelele de întreprindere, însă, serverele de autentificare centralizate externe conduc la obținerea de rezultate mai bune.
- **Criptare** — Unele controlere de acces asigură criptarea datelor transmise de la client la server și înapoi, folosind metode uzuale, cum ar fi *IPSec*. Acest lucru asigură o protecție suplimentară dincolo de ceea ce oferă, în mod obișnuit, standardele de rețele fără fir. Unele dintre aceste caracteristici fac parte, însă, și din browserele Web.
- **Roaming de subrețea** — Pentru a asigura roaming-ul la trecerea de la o rețea la alta, controlerile de acces oferă roaming în *subrețele* fără să mai fie necesară reautentificarea cu sistemul. Ca urmare, utilizatorii pot folosi în continuare aplicațiile lor de rețea, fără să fie necesară vreo întrerupere atunci când se deplasează prin interiorul clădirii. Acest lucru este util îndeosebi pentru rețelele mai mari în care accesul, pentru anumiți utilizatori, va presupune trecerea prin mai multe subrețele.
- **Administrarea lărgimii de bandă** — Deoarece utilizatori dintr-o rețea fără fir împart între ei lărgimea de bandă, este important să existe un mecanism care să prevină acapararea lărgimii de bandă de către anumiți utilizatori. Controlerile de acces realizează această formă de administrare a lărgimii de bandă prin intermediul alocării de profile de utilizator bazate pe nivelele de calitate ale serviciilor (QoS) cerute. Un profil specifică tipurile de servicii (cum ar fi, navigarea pe Web, e-mail, transmisie video) și limitele acceptate pentru performanțe. De exemplu, un vizitator, care nu este abonat și care încearcă să utilizeze o rețea LAN fără fir publică, poate fi clasificat ca aparținând de profilul „vizitator”, profil pentru care s-ar putea asigura numai accesul la informațiile legate de „punctul fierbinte” local. Un abonat, însă, poate avea un alt profil care să-i permită o conexiune de bandă largă la Internet.

Software pentru conectivitatea aplicațiilor

În general, navigarea pe Web și utilizarea e-mail-ului se pot realiza în condiții bune prin intermediul rețelelor fără fir. Este necesară numai instalarea unui browser

și a unui software de e-mail pe *dispozitivul client*. Utilizatorii pot să piardă, din când în când, o conexiune fără fir, însă protocoalele utilizate pentru aceste aplicații relativ simple au capacitatea de a reface conexiunile, în aproape toate situațiile.

În afară de aceste aplicații simple însă, un software pentru conectivitatea aplicațiilor speciale este necesar ca interfață între dispozitivul de calcul al utilizatorului și sistemul final care găzduiește software-ul aplicației sau baza de date. Aplicațiile pot fi un software de administrare de depozit rulând pe un IBM AS/400, o aplicație de modelare aflată pe un sistem UNIX sau un sistem de administrare a timpului rezident pe un vechi sistem mainframe. Bazele de date sunt parte a unui sistem client/server, în care software-ul de aplicație se află, parțial sau în întregime, pe dispozitivul client și comunică cu un sistem de baze de date, cum ar fi Oracle sau Sybase. În aceste cazuri, software-ul pentru conectivitatea aplicațiilor este important, pe lângă punctele de acces și controlerile de acces, în realizarea comunicării dintre dispozitivul de calcul al utilizatorului și software-ul de aplicație sau sistemul de baze de date, localizate pe un server central.

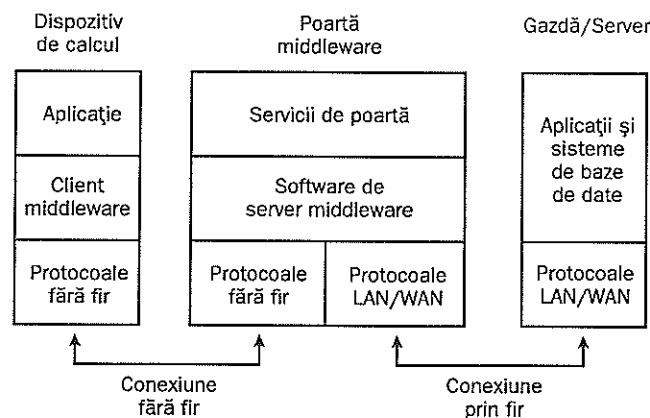
În continuare, sunt enumerate câteva tipuri de software pentru conectivitatea aplicațiilor:

- **Emularea terminalului** — Software-ul de emulare a terminalului rulează pe un dispozitiv de calcul, făcând ca acesta să opereze ca un terminal care oferă o interfață cu utilizatorul relativ simplă pentru software-ul aplicației care rulează pe un alt calculator. Terminalul doar afișează informații pentru utilizator și acceptă intrări remise de software-urile de aplicații. De exemplu, *emulatorul de terminal VT220* comunică cu aplicații care rulează pe gazde UNIX, emulatorul de terminal 5250 lucrează cu sistemele bazate pe IBM AS/400, iar emulatorul de terminal 3270 operează cu mainframe-uri IBM.

Avantajul utilizării emulării de terminal constă în costul său inițial scăzut și în faptul că modificările făcute în aplicație își produc efectul, în mod automat, atunci când utilizatorul se conectează. Însă, este posibil ca sistemele fără fir care utilizează emularea terminalului să nu poată menține conexiuni cu aplicațiile moștenite, care au mesaje de expirare stabilite pe fir mai fiabile. Mesajele de expirare vor întrerupe, în mod automat, dacă nu sesizează desfășurarea unei activități pe dispozitivul client și, urmare, sistemele vor trebui să consume mult timp pentru a recupera informațiile utilizatorilor finali privitoare la căderea conexiunilor incomplete de date. De aceea, implementarea emulării are un efect dezastruos, pe termen lung, asupra costurilor de

- **Conectivitate directă de baze de date** — Conectivitatea directă de baze de date, numită uneori și client/server, cuprinde software de aplicație care rulează pe dispozitivul de calcul al utilizatorului. În această configurație, software-ul de pe dispozitivul utilizatorului final asigură funcționalitatea aplicației și comunică, în general, cu un sistem de baze de date localizat pe un server central. Acest lucru conferă flexibilitate atunci când sunt dezvoltate aplicațiile, deoarece programatorul are un control complet asupra funcțiilor care sunt implementate — nu există constrângeri generate de vreo aplicație moștenită, localizată pe un calculator central. Conexiunile directe de baze de date constituie adesea cea mai bună abordare atunci când este nevoie de flexibilitate în scrierea software-ului de aplicație. Există însă o problemă, legată de faptul că această abordare este dependentă de utilizarea protocolului TCP/IP (Transmission Control Protocol/Internet Protocol), care nu este foarte potrivit pentru comunicațiile prin rețelele fără fir.
- **Middleware fără fir** — Software-ul middleware fără fir asigură comunicații prin intermediar, între dispozitivele de calcul ale utilizatorilor și software-ul de aplicație sau sistemul de baze de date, localizate pe un server (vezi figura 2.5). Middleware-ul — care rulează pe un calculator dedicat (poarta middleware) legat la rețeaua cu fir — procesează pachetele care trec între dispozitivul de calcul al utilizatorului și servere. Software-ul middleware oferă, în primul rând, comunicații eficiente și sigure prin rețeaua fără fir în timp ce menține conexiunile adecvate cu software-ul de aplicație și cu sistemele de baze de date de pe server prin intermediul rețelei cu fir care este mai sigură în funcționare. Uneori, acest lucru este numit persistența sesiunii.

Figura 2.5. Middleware-ul fără fir interconectează eficient aplicații de pe dispozitivele de calcul cu gazde și servere



În continuare, sunt enumerate câteva caracteristici ale produselor middleware:

- **Tehnici de optimizare** — Multe produse middleware includ compresia datelor, pentru a reduce numărul de pachete transmise prin legăturile fără fir. Unele implementări ale middleware folosesc protocoale de comunicații brevet, care conduc la cheltuieli mai mici prin comparație cu protocoalele tradiționale, cum este TCP/IP.
- **Reporniri inteligente** — În cazul rețelelor fără fir, se poate produce o întrerupere neașteptată, în mijlocul transmisiei. Repornirea inteligentă este un mecanism de recuperare care detectează sfârșitul prematur al unei transmisii. Atunci când conexiunea este restabilită, middleware-ul reia transmisia de la punctul în care a survenit întreruperea, nu de la început. Acest lucru evită apariția de erori în aplicațiile care utilizează baze de date.
- **Comasarea de date (data bundling)** — Unele middleware-uri sunt capabile să reunească pachete de date mai mici într-un singur pachet mare, pentru a-l transmite prin rețeaua fără fir, ceea ce poate conduce la scăderea costurilor serviciilor de transmisie pentru WAN-uri. Cum unele servicii de date fără fir taxează utilizatorii pe pachet transmis, comasarea datelor conduce la un cost total mai scăzut.
- **Modificarea configurației ecranelor** — Unele produse middleware mai evoluate permit celor care dezvoltă software-ul să utilizeze instrumente vizuale pentru a modifica și a remodifica porțiuni ale unor ecrane de aplicații existente pentru a le adapta mai eficient la modul de afișare a datelor pe ecranele mai mici ale dispozitivelor de calcul care nu sunt PC-uri, cum ar fi PDA-urile sau scanerele de coduri de bare.
- **Asistarea sistemelor finale** — Middleware-urile fără fir se conectează la o varietate de sisteme finale de aplicații și de sisteme de baze de date. Dacă clienții au nevoie de acces la prea multe aplicații și sisteme de baze de date, middleware-ul fără fir acționează ca un concentrator. De exemplu, un utilizator poate folosi conexiunea middleware pentru a accesa simultan aplicații aflate atât pe un sistem AS/400 cât și pe un sistem UNIX, fără să se preocupe de rularea software-ului adecvat pentru emularea terminalului.



Sistemul de distribuție

O rețea fără fir este rareori complet lipsită de fire. Sistemul de distribuție, care adesea include cabluri, este, în general, necesar pentru a lega împreună punctele de acces, controlerile de acces și serverele. În cele mai multe cazuri, sistemul de distribuție e realizat pe baza popularului Ethernet.

Standardul IEEE 802.3 constituie bazele Ethernet-ului și specifică folosirea protocolului de acces multiplu cu detectarea purtătoarei (în limba engleză: carrier sense multiple access — acronim CSMA) pentru asigurarea accesului printr-un mediu partajat, cum sunt cablurile cu perechi răsucite, cablurile coaxiale sau fibrele optice. CSMA este standardul de acces la mediu folosit în mod predominant astăzi atât pentru rețelele cu fir cât și pentru cele fără fir.

CSMA realizează partajarea unui mediu comun, permițând doar unui singur NIC să transmită informații la un moment dat. Acest lucru este similar cu situația dintr-o ședință în care un participant (ca și o placă de rețea NIC) vorbește numai atunci când ceilalți tac. Acest lucru oferă fiecărei persoane responsabilitate, în sensul că distribuie decizia privitoare la începerea emisie verbale la fiecare persoană. Dacă vorbesc simultan mai multe persoane, apare o coliziune și fiecare dintre aceste persoane trebuie să-și aștepte rândul pentru a repeta ceea ce avea de spus.

În cazul utilizării distribuitoarelor Ethernet, toate dispozitivele de calcul dintr-o rețea trebuie să-și aștepte rândul pentru a folosi mediul. Un comutator Ethernet realizează, însă, mai multe domenii de coliziune, ceea ce asigură posibilitatea transmisiilor simultane între utilizatori pentru a îmbunătăți performanțele rețelei. Pentru rețelele mai mari, dincolo de mărimea unei rețele pentru o locuință sau pentru o mică firmă, puteți fi siguri că trebuie utilizate comutatoarele pentru a optimiza performanțele.

Rețelele Ethernet folosesc cabluri pereche răsucită, cabluri coaxiale sau fibre optice pentru interconectarea dispozitivelor rețelei, cum sunt punctele de acces și alte echipamente de distribuție. Utilizarea cablurilor coaxiale, în vechile LAN-uri cu fir, era comună acum 10 ani, dar astăzi cele mai multe companii folosesc cablurile pereche răsucită sau fibrele optice. Electronic Industries Association (Asociația Industriei Electronice — acronim EIA) și Telecommunications Industry Association (Asociația Industriei Telecomunicațiilor — acronim TIA) prezintă categoria 5 (acronim Cat 5) de cabluri pereche răsucită, ca fiind cel mai comun tip de cablu pereche răsucită utilizat astăzi în rețelele Ethernet.

Cat 5 constă în patru perechi răsucite neecranate de fire, măsura 24, care asigură transmiterea semnalelor Ethernet pe 100 de metri de cablaj. Repetoarele Ethernet pot crește această distanță dacă e necesar, aceasta fiind o metodă de se a ajunge la stație de bază a unei rețele fără fir, aflată la peste 100 de metri de o casetă de comunicații.

Există și alte variante de cabluri pereche răsucită. Categoria 5 îmbunătățită (acronim Cat 5e) utilizează toate cele patru perechi de fire pentru a asigura conectivitate Gigabit Ethernet (1000 Mbps) pe distanțe scurte. Cablurile Cat 5e sunt compatibile cu cele Cat 5. Astăzi sunt disponibile și variantele Cat 6 și Cat 7, care asigură o lărgime de bandă și o distanță de transmisie mai mari și pentru rețelele Gigabit Ethernet bazate pe fire de cupru. Cablurile Cat 7 sunt formate din perechi răsucite ecranate (STP), ceea ce le face ideale pentru instalarea în locații unde există o probabilitate mare de apariție a interferenței electromagnetice.

În continuare, sunt prezentate tipurile comune de cabluri pereche răsucită Ethernet care pot fi utilizate pentru sistemele de distribuție LAN fără fir:

- **10BASE-T** — 10BASE-T este unul dintre straturile fizice 802.3 care specifică o viteză de transmisie a datelor de 10 Mbps. Un cablu 10BASE-T tipic folosește două dintre cele patru perechi de fire dintr-un cablu Cat 5 pentru transmisia și recepția datelor. Fiecare capăt al cablului posedă conectori RJ-45 (puțin mai mari decât conectorii telefonici RJ-11 utilizați în America de Nord).

Avantajul existenței unei perechi de fire în plus constă în faptul că aceasta este disponibilă pentru alte utilizări, cum ar fi Power-over-Ethernet (PoE). Acesta este un mecanism prin care un modul alimentează în curent continuu un cablu Cat 5, permițându-vă să furnizați, de la caseta de comunicații, energia necesară pentru punctele de acces. PoE elimină adesea necesitatea instalării de către un electrician a unor alimentări electrice noi la fiecare punct de acces. Pentru rețelele mai mari, trebuie categoric luată în considerare utilizarea PoE.

- **100BASE-T** — Un alt strat fizic 802.3, 100BASE-T asigură viteze de transmisie a datelor de 100 Mbps. Similar cu 10BASE-T Ethernet, 100BASE-T utilizează perechi de fire răsucite, existând următoarele opțiuni:
 - 100BASE-TX utilizează două perechi de fire din cablul Cat 5;
 - 100BASE-T4 utilizează patru perechi de fire din cablul Cat 3, mai vechi și de o calitate inferioară.

Majoritatea implementărilor din ziua de azi folosesc cablaje 100BASE-TX. Ca și în cazul 10BASE-T, PoE poate folosi perechea de fire neutilizată. 100BASE-T4 a fost versiunea populară, pentru asigurarea vitezelor de transmisie de 100 Mbps prin cablaje Cat 3 (de tip mai vechi), des folosită la începutul anilor 1990.

- **Fibrele optice** – Fibrele optice sunt mai scumpe decât perechile de fire răsucite, însă pot fi eficiente din punctul de vedere al costurilor pentru că asigură viteze de transfer de ordinul gigabiților pe distanțe de până la doi kilometri. În locul utilizării abordării tradiționale semnal-electric-prin-fir-de-cupru, fibrele optice folosesc pulsuri de lumină transmise prin fâșii subțiri de sticlă sau plastic. Acest lucru duce la un cablu cu fibre optice neafectat de interferența electromagnetică, ceea ce îl face să fie prețios în situațiile în care emisiile electronice sunt un motiv de preocupare. În plus, monitorizarea pasivă a transmisiilor de date prin fibre optice este aproape imposibil de realizat, ceea ce le face pe acestea să fie un mediu mai sigur decât perechile de fire răsucite.

În cazul utilizării în LAN-urile fără fir, fibrele optice sunt o soluție posibilă pentru transmisia la un punct de acces aflat la peste 100 de metri de caseta de comunicații. Însă, acest lucru presupune, utilizarea unei perechi de transceivere scumpe, care transformă semnalele electrice în lumină (și invers). O problemă legată de utilizarea fibrelor optice este cea privitoare la conectarea cap la cap a segmentelor de cablu optic. Utilizarea materialelor plastice sau a sticlei presupune un aliniament precis. Veți avea nevoie de instrumente speciale și de o pregătire specială pentru a realiza cabluri cu fibre optice folositoare. Va trebui să cumpărați cabluri cu fibre tăiate în prealabil, pentru a evita probleme dificil de rezolvat.

Sistemele de administrare

Ca și în cazul altor tipuri de rețele, rețelele fără fir de întreprindere presupun un management eficient pentru a putea asigura necesitățile utilizatorului, pe parcursul existenței rețelei. Un sistem de management al rețelei, care implică atât personal cât și instrumente software, satisface aceste cerințe. În continuare sunt prezentate funcțiile care trebuie asigurate de către sistemul de management al rețelei.

Protecție/securitate

Elementul securitate presupune mecanisme care evită periclitatea sau distrugerea resurselor rețelei, cum ar fi sistemele de baze de date sau mesaje e-mail. Acest lucru

presupune întărirea politicilor de securitate pentru configurarea rețelei fără fir într-un mod care să contracareze aspectele legate de propagarea semnalelor prin rețeaua fără fir. De exemplu, politicile pot specifica utilizarea unui anumit tip de criptare pentru a se asigura că o persoană răuvoitoare nu poate recepționa și decoda mesajele e-mail care sunt transmise între utilizator și un punct de acces. Veți găsi mai multe detalii legate de metodele de protejare a rețelelor fără fir în capitolul 8, intitulat *Securitatea rețelelor fără fir: protejarea resurselor de informații*.

Asistența la birou

Asistența la birou (în limba engleză: help desk) asigură primul nivel în sprijinirea utilizatorilor. Un utilizator care are dificultăți cu o conexiune fără fir trebuie să știe cum poate solicita asistența de birou. Utilizatorii au adesea probleme legate de asocieri sau de variații ciudate ale performanțelor.

Personalul asistenței de birou este capabil să rezolve probleme simple legate de conexiune, cum ar fi asistarea utilizatorului la configurarea unei plăci radio și a sistemului de operare pentru a fi în acord cu politicile specifice rețelei fără fir. Asistența de birou trebuie să poată comunica cu funcțiile de asistență mai avansate, cum sunt întreținerea și (re)proiectarea, pentru a rezolva probleme mai complexe, care sunt evidențiate prin contactul cu utilizatorii.

Managementul configurației

Managementul configurației constă în controlul modificărilor făcute în arhitectura rețelei fără fir și în sistemul instalat. Modificările pot consta în instalarea sau mutarea punctelor de acces, modificarea parametrilor punctelor de acces și actualizarea hardware și software. Datorită naturii dinamice a rețelelor fără fir, modificările se produc mai des decât în cazul rețelelor cu fir.

Toate propunerile de modificare a unei rețele fără fir de întreprindere, care au impact asupra performanțelor sau a securității, trebuie verificate. Verificarea permite companiei să ia în considerație implicațiile relevante care presupun costuri suplimentare și utilizarea de resurse. Compania trebuie să realizeze un proces independent de verificare a proiectului, care evaluează fiecare soluție de rețea fără fir propusă și verifică conformitatea cu o arhitectură generală și cu elementele de asistență. Verificarea va trebui să includă, de exemplu, o revizuire a poziționării punctelor de acces, a canalelor de radio frecvență alocate și a setărilor de securitate.

Monitorizarea rețelei

Monitorizarea rețelei presupune evaluarea continuă a diferitelor caracteristici ale rețelei fără fir, incluzând utilizarea punctelor de acces și rutele traficului utilizatorului prin sistemul de distribuție. Acest lucru joacă un rol cheie în managementul anticipativ al rețelei fără fir, pentru a putea asigura funcționarea în cazul unei creșteri a numărului de utilizatori și pentru a rezolva problemele înainte ca acestea să afecteze performanțele sau securitatea rețelei.

O companie trebuie să evalueze în permanență gradul de utilizare al stațiilor de bază pentru a dimensiona corespunzător rețeaua pe măsură ce traficul utilizatorilor se modifică. Stațiile de bază se manifestă ca o măsură care indică dacă sunt necesare noi stații de bază, noi controlere de acces sau o mărire a lărgimii de bandă pentru Internet. O problemă specifică a rețelelor fără fir este aceea că administratorul de rețea poate să nu observe că o stație de bază este inoperantă de un anumit timp.

În majoritatea cazurilor, zonele acoperite de stațiile de bază se suprapun, iar utilizatorii vor fi preluați de o altă stație de bază, la o performanță mai scăzută, dacă punctul de acces inițial nu este disponibil. În acest caz, instrumentele de monitorizare ale rețelei vor observa imediat întreruperea și vor alerta persoana potrivită care se ocupă de întreținerea rețelei. Dacă este posibil, compania trebuie să integreze funcțiile de monitorizare ale rețelei fără fir în instrumente care sunt deja utilizate în rețeaua de întreținere existentă. Acest lucru simplifică asigurarea asistenței operaționale.

Raportarea

Raportarea oferă informații privitoare la aspecte variate ale rețelei fără fir, incluzând statistici legate de gradul de utilizare, notificări privitoare la alarmele de securitate și informații legate de performanțe. Aceste rapoarte sunt necesare administratorilor de rețea pentru a evalua eficient funcționarea rețelei și pentru a lua decizii privitoare la schimbări. Această raportare trebuie să indice, ca un minim acceptabil, potențialele breșe în sistemul de securitate, punctele de acces neoperaționale și gradul de utilizare. Acest tip de informații trebuie să fie disponibil pentru toate funcțiile de asistență operațională, cum sunt asistența de birou, întreținerea și reproiectarea.

Reproiectarea

Elementele de reproiectare oferă asistență tehnică avansată pentru reproiectarea rețelelor fără fir pentru a putea include tehnică nouă și pentru a rezolva problemele legate de asigurarea unor performanțe reale și a unei securități reale. În mod obișnuit, compania sau grupul care a proiectat inițial rețeaua fără fir va realiza funcțiile de reproiectare. Funcțiile de reproiectare trebuie să revadă și să verifice conformitatea dintre proiecte și modelul arhitectural general. În plus, grupul de reproiectare va trebui să monitorizeze în permanență evoluția tehnicilor și a produselor legate de rețelele fără fir pentru a asigura evoluția efectivă a sistemului către o creștere a gradului de utilizare a rețelei.

Întreținerea

Întreținerea se referă la repararea și configurarea rețelei fără fir, incluzând înlocuirea antenelor distruse, setarea canalelor la punctele de acces și reevaluarea propagării undelor radio. Anumite sarcini de întreținere pot rezulta din asistența acordată funcției de reproiectare. De exemplu, proiectanții pot decide necesitatea instalării unui punct de acces suplimentar într-o zonă în care este necesară realizarea acoperirii de către rețea. În acest caz, personalul de întreținere va instala punctul de acces în locația stabilită de proiectanți.

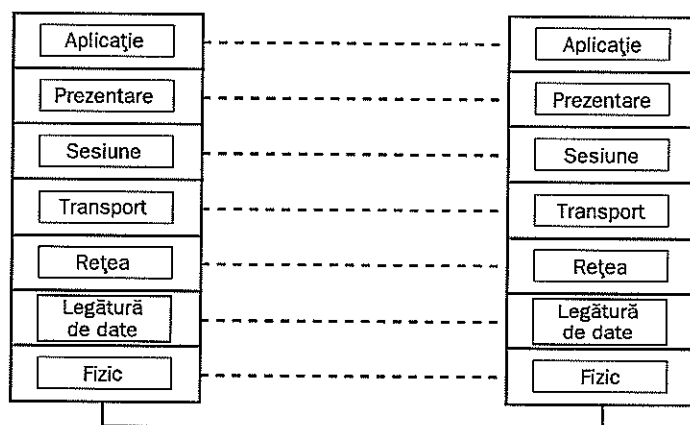
O sarcină importantă în întreținerea unei rețele fără fir constă în actualizarea periodică a hardware-ului și software-ului din punctele de acces. Acest lucru asigură funcționarea punctelor de acces cu ultimele caracteristici înglobate și eliminarea defectelor, ceea ce maximizează performanțele și securitatea rețelei. Prin urmare, o companie trebuie să programeze actualizări regulate ale hardware-ului și software-ului, pe măsură ce sunt disponibile noi versiuni.

Echipa de întreținere trebuie, de asemenea, să efectueze periodic teste de acoperire pentru a se asigura că punctele de acces acoperă corespunzător locațiile, la nivele adecvate de performanță. Acest lucru este necesar atunci când compania modifică structura locației (clădirii), ceea ce implică modificări ale caracteristicilor de propagare ale undelor radio. Dacă sunt descoperite discrepanțe, echipa de întreținere trebuie să raporteze cele observate echipei de reproiectare pentru a se găsi o rezolvare.

Arhitectura rețelei fără fir

Arhitectura rețelei definește protocoalele și componentele necesare pentru a satisface cerințele aplicațiilor. Un standard popular pentru ilustrarea arhitecturii este modelul de referință cu șapte strate OSI (Open System Interconnect), dezvoltat de către Organizația Internațională pentru Standardizare (ISO). OSI specifică un set complet de funcții de rețea, grupate în straturi (vezi figura 2.6), care sunt localizate în fiecare componentă a rețelei. Modelul de referință OSI este un model potrivit și pentru reprezentarea diverselor standarde și interoperabilități ale rețelelor fără fir.

Figura 2.6. Straturile modelului de referință OSI reprezintă toate funcțiile unei rețele



Straturile OSI asigură următoarele funcționalități ale rețelei:

- **Stratul 7 — stratul aplicație:** Stabilește comunicațiile între utilizatori și furnizează serviciile de comunicații de bază cum sunt transferul de fișiere și e-mail. Exemple de software-uri care rulează în acest strat sunt Simple Mail Transfer Protocol (SMTP), HyperText Transfer Protocol (HTTP) și File Transfer Protocol (FTP).
- **Stratul 6 — stratul prezintăre:** Negociază sintaxa transferului de date pentru stratul aplicație și realizează conversii între diferite formate de date, dacă acest lucru este necesar. De exemplu, acest strat poate traduce codul de reprezentare a datelor atunci când se comunică cu un sistem aflat la distanță, fabricat de un alt producător.

- **Stratul 5 — stratul sesiune:** Stabilește, administrează și încheie sesiunile dintre aplicații. Middleware-urile fără fir și controlerele de acces asigură această formă de conectivitate prin rețelele fără fir. Dacă rețeaua fără fir sesizează interferențe, funcțiile stratului sesiune vor suspenda comunicațiile până când interferențele dispar.
- **Stratul 4 — stratul transport:** Asigură mecanismele necesare pentru stabilirea, întreținerea și închiderea corectă a circuitelor virtuale, ascunzând, totodată, detaliile de implementare față de straturile superioare. În general, aceste circuite sunt conexiuni realizate între aplicațiile de rețea de la un capăt la celălalt al circuitului de comunicație (cum ar fi între un browser Web de pe un laptop și o pagină Web de pe un server). Protocoale cum este *Transmission Control Protocol (TCP)* operează în acest strat.
- **Stratul 3 — stratul rețea:** Asigură direcționarea pachetelor prin rețea, de la sursă până la destinație. Direcționarea realizează transmisia pachetelor de date în direcția care le conduce la o anumită destinație. Protocoale cum ar fi Internet Protocol (IP) operează în acest strat.
- **Stratul 2 — stratul legătură de date:** Asigură mediul de acces, sincronizarea și controlul erorilor de transmisie între două entități. În cazul rețelelor fără fir, acest lucru implică, adesea, coordonare accesului la mediul aerian comun și recuperarea erorilor care pot să apară în date pe parcursul propagării de la sursă la destinație. Majoritatea tipurilor de rețele fără fir posedă o metodă comună de realizare a funcțiilor stratului legătură de date, independentă de metoda efectivă de transmisie.
- **Stratul 1 — stratul fizic:** Asigură transmisia efectivă a informației prin mediu. Straturile fizice includ undele radio și lumina infraroșie.

Combinarea straturilor unei arhitecturi de rețea definește funcționalitatea rețelei fără fir, însă rețelele fără fir implementează direct doar straturile inferioare ale modelului. O placă de rețea NIC fără fir, de exemplu, implementează funcții ale stratului fizic și ale stratului legătură de date. Alte componente ale rețelei (cum ar fi middleware-ul fără fir) oferă, însă, funcții implementate de stratul sesiune. În unele cazuri, adăugarea unei rețele fără fir poate avea impact doar asupra straturilor inferioare, dar trebuie acordată atenție și straturilor superioare pentru a se asigura faptul că aplicațiile operează cu eficacitate în prezența avariilor rețelei fără fir.

Fiecare strat al modelului OSI acordă asistență straturilor de deasupra lui. De fapt, straturilor inferioare par, adesea, a fi transparente pentru straturilor de deasupra. De exemplu, TCP, care operează în stratul transport, stabilește conexiuni cu aplicațiile aflate la distanță, pe un calculator gazdă, fără cunoștința faptului că straturilor inferioare se ocupă de sincronizare și de semnalizare.

Așa cum se arată în figura 2.6, protocoalele din fiecare strat comunică prin rețea cu respectivul strat pereche. Transmisia efectivă de date apare, însă, în stratul fizic. Prin urmare, arhitectura permite realizarea unui proces de stratificare prin care fiecare strat introduce (încapsulează) informațiile protocolului său în cadre care sunt plasate în interiorul cadrelor straturilor inferioare. Cadru transmis de stratul fizic conține, de fapt, cadrele din toate straturilor superioare. La destinație, fiecare strat transferă cadrele adecvate straturilor superioare pentru a facilita acțiunea protocolului între straturile pereche.

Semnalele care transmit informația

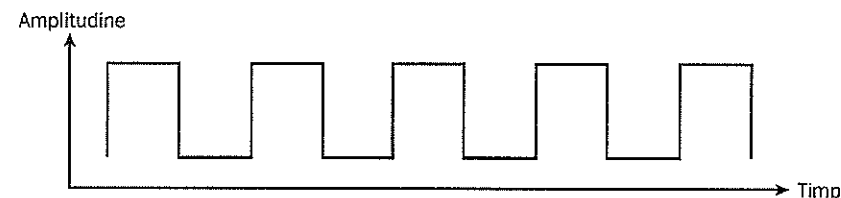
Datele sunt tipul de informație pe care rețeaua o stochează într-un calculator sau o preia de la acesta. Prin urmare, rețelele fără fir transferă datele de la un calculator la altul. Aceste date pot include mesaje e-mail, fișiere, pagini Web, secvențe video, muzică și conversații realizate prin voce.

Sistemele de comunicații — cum sunt rețelele fără fir — simbolizează datele folosind coduri pe care semnalele electrice, cele radio sau cele luminoase le pot reprezenta cu eficacitate. Semnalele transportă informațiile prin sistem de la un punct la altul. Semnalele pot fi digitale sau analogice, în funcție de localizarea lor în sistem.

Semnalele digitale

Semnalele digitale, care sunt regăsite în calculatoare, variază în trepte de amplitudine în funcție de timp (vezi figura 2.7). Semnalele digitale sunt de obicei binare (două stări); de aceea se face uzual referire la semnal ca fiind o serie de cifre binare (biți) sau date binare. Circuitele digitale din interiorul calculatorului stochează și procesează cu ușurință aceste semnale digitale, în forma lor binară.

Figura 2.7. Semnalele digitale sunt ideale pentru utilizarea în calculatoare



Sistemul binar este un sistem care folosește doar cifrele 0 și 1 pentru a reprezenta numerele. Conversiile din sistemul de numerație zecimal, mai familiar, în cel binar, sunt ușor de realizat, iar calculatoarele pot stoca rapid numerele binare. În cazul unor protocoale, valorile binare din interiorul unui cadru de date reprezintă informații specifice protocolului respectiv.

Unul dintre avantajele semnalelor digitale este faptul că permit cu ușurință regenerarea semnalului. Atunci când semnalul se propagă prin mediul aerian, poate întâlni zgomote sau interferențe care pot modifica aparența de „formă de valuri” a semnalului. Pentru a curăța și regenera semnalul, circuitele digitale pot detecta dacă un puls digital este prezent la o anumită perioadă de timp și pot crea un nou puls care este identic cu cel trimis inițial. Prin urmare, un semnal digital poate fi transmis pe distanțe mari prin intermediul repetărilor periodice, păstrându-se integritatea informației. Acest lucru nu este posibil în cazul semnalelor analogice.

Din motive de securitate, este adesea necesar ca semnalele să fie criptate și apoi decriptate la destinație. Acest proces este simplu în cazul semnalelor digitale, deoarece tot ce trebuie făcut este să fie rearanjați biții utilizând un anumit tip de proces, bazat pe o cheie secretă. Atunci când datele ajung la destinație, un dispozitiv poate folosi aceeași cheie pentru a decripta datele.

În continuare, sunt definite caracteristicile importante ale semnalelor digitale:

- **Viteza (de transfer a) datelor** (în limba engleză: **data rate**) — Viteza datelor reprezintă viteza cu care semnalele digitale transferă datele printr-o rețea fără fir. Prin urmare, viteza de date a semnalelor digitale oferă o oarecare înțelegere cu privire la cât timp va dura transmiterea datelor de la un punct la altul și, totodată, identifică valoarea *lărgimii de bandă* pe care mediul trebuie să o furnizeze pentru a asigura transmisia eficientă a semnalului. Viteza datelor

semnalului este egală cu numărul total de biți transmiși raportați la timpul necesar pentru transmiterea acestora. Unitatea comună de măsură pentru viteza datelor este biți pe secundă (bps). Ca un exemplu, să considerăm un semnal care transferă 1 000 000 de biți într-o secundă. Viteza datelor este $1\,000\,000/1 = 1\,000\,000$ bps (sau 1 Mbps).

- **Transferul** (în limba engleză: **throughput**) — Transferul este o mărime similară cu viteza datelor; însă calcularea transferului exclude, în general, biții adăugați de protocoalele de comunicații peste datele utilizatorului. Nu există standarde pentru definirea transferului, însă acesta include, de regulă, doar informațiile trimise efectiv prin rețea. Prin urmare, transferul oferă o cale mai exactă de reprezentare a performanței reale și a eficienței reale a rețelei. Acest lucru face ca transferul să fie important atunci când se compară rețelele fără fir, deoarece este legat direct de performanță. Cu cât transferul este mai mare, cu atât performanța este mai înaltă.

Viteza datelor unei rețele LAN fără fir poate fi, de exemplu, de 11 Mbps, dar transferul poate fi de numai 5 Mbps. După îndepărtarea surplusului — antetele cadrelor, câmpurile pentru verificarea erorilor, cadrele de confirmare și retransmisiile datorate erorilor — transferul de informații rezultat este considerabil mai scăzut. Pe măsură ce numărul de utilizatori crește, crește concurența la împărțirea mediului, ceea ce conduce la o scădere chiar mai pronunțată a transferului, deoarece dispozitivele de calcul (NIC-urile fără fir, pentru a fi mai exact) trebuie să aștepte mai mult înainte de a transmite datele. Această întârziere, care este o formă de surplus, poate reduce semnificativ transferul.

În cazul rețelelor fără fir se obișnuiește să se spună că sistemul transmite biți de date. În realitate, o rețea fără fir convertește semnalele digitale binare în semnale analogice înainte de a le transmite prin mediul aerian.

Semnalele analogice

Un *semnal analogic*, așa cum este prezentat în figura 2.8, este un semnal în care amplitudinea variază continuu în timp. În majoritatea cazurilor, mediul natural produce semnale de formă analogică. Exemple de astfel de semnale sunt lumina și vocea umană. Semnalele produse de om, cum ar fi undele radio, au tot formă analogică.

Figura 2.8. Semnalele analogice poartă informația prin mediul aerian



La începuturile comunicațiilor electronice, majoritatea sistemelor procesau semnalele în formă analogică, în primul rând pentru că intrările lor erau informații care veneau de la oameni. Un semnal analogic posedă amplitudine, măsurată în unități de tensiune sau de putere, și frecvență (măsurată în număr de cicluri pe secundă, numiți și *Hertzi*). În general, rețelele fără fir utilizează semnale analogice la frecvență de 2,4 GHz, care se află în banda de frecvențe numită undă radio. Există câteva metode diferite de a descrie amplitudinea semnalelor transmise fără fir. Puteți găsi detalii legate de semnalele analogice transmise fără fir în capitolul 3.

Fluxul de informații printr-o rețea fără fir

Desigur că motivul pentru care este folosită o rețea fără fir este acela că asigură un flux de informații, de la un punct la un altul, fără a utiliza firele. În timpul transferului prin rețea, informația își schimbă forma pentru a traversa în mod eficient rețeaua. Funcțiile specifice legate de transferul informației, cum ar fi accesul la mediu și controlul erorilor, sunt comune pentru diversele tipuri de rețele fără fir.

Punctele finale ale fluxului de informații

Fluxul de informații începe și se termină, adesea, la utilizatori. Un om de afaceri poate trimite un mesaj e-mail dintr-un aeroport, un medic poate vizualiza fișa medicală a unui pacient de pe un PDA fără fir sau un funcționar de depozit poate introduce cantitățile de produse printr-un terminal, ca parte a administrării inventarului. Atunci când utilizatorii comunică informații, ei pot utiliza text, imagini, voce sau secvențe video prin intermediul unui dispozitiv de calcul.



Inițial, aceste informații pot să fie numai gânduri în mintea cuiva, gânduri pe care utilizatorul le introduce într-o formă de informație, cum ar fi textul sau vocea, și pe care dispozitivul de calcul le stochează ca date. În cazul utilizatorilor umani, informația se află, în general, în formă analogică; informația trebuie să fie un semnal digital atunci când este transferată unui utilizator care nu este uman, cum ar fi un robot sau un dispozitiv de calcul.

Introducerea, stocarea și afișarea informațiilor

Fluxul de informații pornește de la un utilizator printr-un dispozitiv de calcul care permite introducerea informațiilor prin intermediul unei tastaturi, a unui microfon sau a unei camere video. Metode mai noi permit și introducerea informației pe baza mișcărilor ochilor sau pe baza undelor cerebrale. Semnalele analogice reprezintă aceste informații.

Însă, înainte ca dispozitivul de calcul să poată stoca informațiile, sistemul trebuie să convertească semnalele de informație analogice în forma digitală, care este potrivită pentru dispozitivul de calcul. Convertori analogic-digitali (A/D) fac acest lucru posibil. Circuite speciale eșantionează semnalul analogic, rezultând pulsuri cu amplitudini care reprezintă numere binare. La fel, convertori digital-analogici (D/A) transformă semnalele digitale în unele analogice, ca parte a procesului de prezentare a informației pentru utilizator.

În interiorul unui dispozitiv de calcul, coduri speciale reprezintă informațiile ca date. Codul ASCII (American Standard Code for Information Interchange — Codul standard american pentru schimbul de informații), de exemplu, reprezintă caracterele alfabetului englez prin numere. Calculatorul stochează aceste numere ca date. Ca un exemplu, codul ASCII (în format hexazecimal) pentru majuscula „A” este 41, iar pentru litera mică „h” este 68. Majoritatea calculatoarelor folosesc codificarea ASCII pentru a reprezenta informația aflată sub formă de text, în numere binare, care utilizează numai cifrele 0 și 1. Alte tehnici de codificare simbolizează informațiile audio și video.

Legătura cu mediul aerian

După ce utilizatorul instruește dispozitivul de calcul pentru ca acesta să transmită informația prin rețeaua fără fir, dispozitivul de calcul negociază o

conexiune cu calculatorul destinat aflat la distanță, ceea ce implică utilizarea funcțiilor straturilor transport și sesiune. După stabilirea conexiunii, dispozitivul de calcul livrează datele în formă digitală NIC-ului fără fir. În general, NIC-ul fără fir transmite cadrul care conține informațiile, cadru care este în conformitate cu un standard specific, cum ar fi IEEE 802.11, către NIC-ul fără fir aflat la distanță, într-un dispozitiv de calcul sau într-un punct de acces.

NIC-ul care transmite convertește datele într-un semnal de radio frecvență analogic sau în unde luminoase înainte de a le transmite prin antenă. Această conversie necesită modularea semnalului, ceea ce implică conversia semnalului din forma digitală în cea analogică. Capitolul 3 descrie particularitățile acestui proces. După modulare, semnalul se propagă prin mediul aerian până la NIC-ul receptor, care demodulează și apoi procesează semnalul recepționat, înainte de a livra datele straturilor superioare ale arhitecturii de rețea.

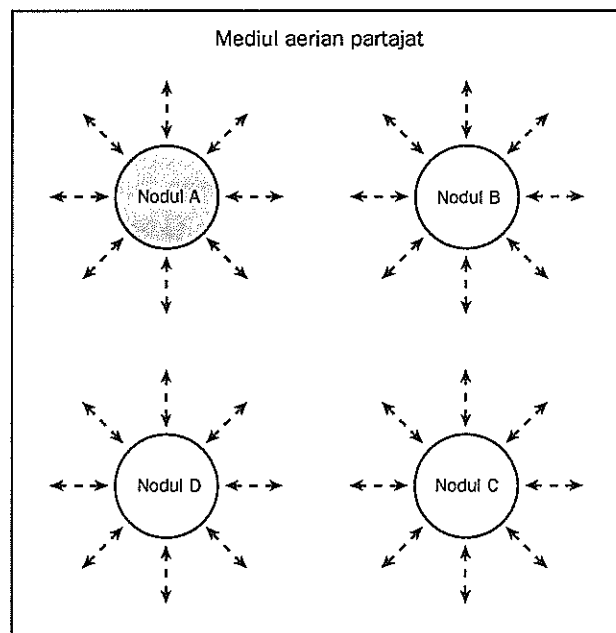
Accesul la mediu

Un aspect important al transmisiei datelor prin rețeaua fără fir se referă la *accesul la mediu*, o funcție a stratului legătură de date care cuprinde protocoalele pe care trebuie să le urmeze toate NIC-urile fără fir. Aceste protocoale asigură coordonarea transmisiei datelor de către NIC-urile fără fir, mai ales atunci când numai o singură placă de rețea NIC poate transmite la un anumit moment dat. Fără acest mecanism, s-ar produce coliziuni.

Ca și în cazul rețelelor cu fir, CSMA este protocolul uzual pentru accesul la mediu folosit de rețelele fără fir. CSMA implementează un protocol de tipul ascultă-înainte-să-vorbești pentru a regulariza accesul distribuit la un mediu comun. Prin utilizarea CSMA, fiecare NIC fără fir are capacitatea de a sesiza transmisiile pornite de la alte dispozitive.

Dacă nodul A are de transmis date, pentru început va verifica — va sesiza — dacă oricare dintre celelalte noduri transmite date (vezi figura 2.9). Dacă mediul este liber — nu se „aude” nici o transmisie — nodul A va transmite un cadru de date. Dacă nodul A sesizează transmisiile de la un alt nod, nu va porni transmisia și va aștepta o perioadă de timp, înainte de a verifica din nou canalul. Operațiunea de verificare continuă până când nodul reușește să transmită cadrul cu date.

Figura 2.9. Nodul A face parte dintr-o rețea fără fir ipotetică în care fiecare nod își așteaptă rândul pentru a transmite datele



În cazul utilizării CSMA, coliziunile pot totuși să apară, chiar dacă fiecare nod verifică canalul de transmisie înainte de a începe să trimită datele. Motivul pentru care se petrece acest lucru este existența întârzierilor datorate propagării semnalelor între noduri. Transmisia care pornește dintr-un anumit nod nu blochează transmisiile din toate celelalte noduri până când nu ajunge la toate nodurile.

De exemplu, nodul B începe să transmită un semnal. Nodul A trebuie să transmită și el un cadru. Acesta verifică mediul și îl găsește liber, deoarece semnalul de la nodul B nu a ajuns încă la nodul A din cauza întârzierii de propagare. Prin urmare, nodul A sesizează că mediul nu e utilizat și începe transmisia. În momentul următor se produce coliziunea între cele două cadre, ceea ce generează erori semnificative în ambele cadre de date. Ambele noduri trebuie să-și retransmită cadrele.

CSMA oferă un acces asincron la mediu, ceea ce înseamnă că nu poate exista garanția că o anumită placă de rețea NIC va putea să acceseze mediul și să transmită datele într-un anumit interval de timp. De aceea, în cazul utilizării CSMA, transmisiile pachetelor nu sunt permanente. Acest lucru creează o problemă pentru transmisiile de informații în timp real, cum sunt vocea și secvențele video, deoarece e posibil

ca rețeaua să nu poată livra tranșele de informații suficient de regulat pentru a satisface cerințele de calitate. În acest caz, sunt necesare funcții QoS și o rată de transfer mai înaltă pentru a îmbunătăți performanțele.

Controlul erorilor

Semnalele care transmit informații pot suferi erori de biți atunci când se propagă prin mediul aerian. Zgomotul și interferențele din zona în care se află rețeaua fără fir produc aceste erori. Prin urmare, NIC-urile fără fir implementează mecanisme de control al erorilor care detectează și corectează erorile biților.

Zgomotul produs de radiația solară și de dispozitivele realizate de om poate afecta semnalele folosite la transmisia fără fir a informațiilor, iar acesta este prezent întotdeauna. Însă, *zgomotul de fond* este de obicei suficient de scăzut pentru ca receptoarele să fie capabile să distingă semnalul de informație de zgomot. Pe distanțe mari însă, atenuarea poate reduce puterea semnalului de informații până la un nivel care se află sub nivelul zgomotului de fond, și atunci încep să apară erorile de biți.

De regulă, zgomotul care produce alterarea biților în rețelele fără fir are sau formă gaussiană, sau formă de impuls. Teoretic, amplitudinea zgomotului gaussian este constantă în spectrul de frecvențe și, în mod normal, generează erori aleatoare, care sunt independente între ele. Zgomotul impuls, care este cel mai periculos, este caracterizat prin lungi intervale de „tăcere” urmate de un impuls de mare amplitudine. Acest zgomot este produs de cauze naturale — cum ar fi fulgerul — precum și de dispozitive realizate de om. Zgomotul impuls este responsabil de majoritatea erorilor apărute în sistemele de comunicații digitale și provoacă, în general, apariția de erori grupate, dependente unele de altele. Această distorsiune este cunoscută sub numele de eroare impuls (sau explozie).

Tehnicile de control al erorilor reduc în mare măsură numărul erorilor de transmisie. Erorile de biți pot să apară totuși atunci când cadrele de date călătoresc prin mediul aerian, însă mecanismele de control al erorilor corectează aceste erori. Ca urmare, transmisia informației prin mediul aerian pare a fi lipsită de erori pentru protocoalele din straturile superioare și pentru utilizatori.

Cele două tipuri fundamentale de control al erorilor sunt solicitarea automată a repetării (în limba engleză: automatic repeat-request — acronim ARQ) și corecția erorilor în avans (în limba engleză: forward error correction — acronim FEC).

În cazul ARQ, care operează în stratul legătură de date, NIC-ul fără fir receptor detectează erorile și utilizează o cale de feedback către NIC-ul fără fir transmițător, pentru a-i solicita acestuia retransmisia cadrelor care au avut erori de biți. Există două evenimente principale care pot să apară la corectarea erorilor cu ARQ. În primul rând, un cadru recepționat trebuie verificat la receptor pentru posibile erori, iar apoi transmițătorul trebuie anunțat pentru a putea retransmite cadrele recepționate cu erori. În unele protocoale, cum este și 802.11, receptorul transmite o confirmare la transmițător, dacă cadrul recepționat nu prezintă erori. Absența unei confirmări indică transmițătorului că trebuie să retransmită cadrul respectiv.

Există două abordări pentru retransmiterea blocurilor de date cu erori:

- ARQ „oprește-te și așteaptă“;
- ARQ continuu.

ARQ „oprește-te și așteaptă“

În metoda de transmisie „oprește-te și așteaptă“, NIC-ul expeditor transmite un bloc de date iar apoi se oprește și așteaptă o confirmare, de la NIC-ul receptor, privitoare la faptul că un anumit cadru este acceptabil sau nu. Dacă expeditorul primește o înfirmare, va retransmite cadrul transmis anterior. NIC-ul expeditor va transmite cadrul următor după ce va primi o confirmare de la NIC-ul receptor. Standardul 802.11 specifică această formă de control al erorilor.

Un avantaj al metodei ARQ „oprește-te și așteaptă“ este acela că nu necesită multă memorie la NIC-ul expeditor și la cel receptor. Cadrele transmise și încă neconfirmate trebuie stocate doar la expeditor (pentru cazul în care trebuie retransmise). Pe de altă parte, metoda ARQ „oprește-te și așteaptă“ devine inefficientă pe măsură ce crește întârzierea de propagare între sursă și destinatar. De exemplu, în cazul datelor transmise prin legăturile prin satelit se produc întârzieri de ordinul câtorva sute de milisecunde; de aceea, este necesar ca blocurile de date să aibă lungimi mari pentru a se menține o viteză efectivă de transmisie a datelor rezonabilă. Problema este că, în cazul blocurilor mari de date, probabilitatea de apariție a erorilor într-un anumit bloc este mai mare. În concluzie, vor fi necesare retransmisii mai dese, iar transferul care rezultă va avea valori mai scăzute.

ARQ continuu

O cale de a îmbunătăți transferul în cazul legăturilor mai lungi este utilizarea metodei ARQ continuu. În cazul acestui tip de ARQ, expeditorul transmite continuu

blocuri de date până când NIC-ul receptor detectează o eroare. NIC-ul expeditor este capabil, de regulă, să transmită un anumit număr de cadre și să țină o evidență a acestor cadre transmise. Îndată ce NIC-ul receptor detectează un bloc cu erori, el va transmite un semnal înapoi la NIC-ul expeditor, solicitând retransmisia cadrului cu erori. Atunci când expeditorul primește solicitarea de a retransmite un anumit cadru, câteva cadre consecutive trebuie să fi fost deja transmise datorită întârzierilor de propagare între expeditor și receptor.

În cazul ARQ continuu, NIC-ul expeditor poate retransmite cadrele în mai multe moduri. O metodă constă în preluarea de către expeditor a cadrului respectiv din memoria sa și retransmisia lui, ca și a cadrelor care urmează după acesta. Aceasta se numește tehnica „întoarcerea la n“ și poate fi mai eficientă decât ARQ „oprește-te și așteaptă“, pentru că folosește mai bine lărgimea de bandă a canalului. O problemă este că atunci când n – numărul de cadre pe care expeditorul le-a transmis după cadrul cu erori — plus unu — ajunge să fie mare, metoda devine inefficientă. Acest lucru se întâmplă deoarece retransmisia unui singur cadru cu erori presupune și retransmisia unui număr mare de cadre bune, ceea ce micșorează transferul.

Tehnica „întoarcerea la n“ este utilă în aplicațiile în care receptorul are puțină memorie disponibilă, pentru că acesta trebuie să memoreze doar un singur cadru, presupunând că nu este necesară livrarea cadrelor în ordine. Atunci când NIC-ul receptor respinge un cadru cu erori — adică atunci când transmite un mesaj de înfirmare — nu trebuie să stocheze nici unul dintre cadrele care urmează, pentru o posibilă reordonare, în timp ce așteaptă retransmisia. Aceasta deoarece toate aceste cadre vor fi și ele retransmise.

O alternativă la tehnica „întoarcerea la n“ este o metodă care retransmite selectiv numai cadrele care au avut erori și reia transmisia normală de la punctul de dinaintea primirii notificării privitoare la existența unui bloc de date cu erori. Aceasta este abordarea „repetare selectivă“. Repetarea selectivă este în mod evident mai bună decât „întoarcerea la n“ în termeni de transfer, deoarece NIC-ul expeditor retransmite numai blocurile de date care au prezentat erori; însă, receptorul trebuie să fie capabil să stocheze un număr de cadre de date, dacă acestea urmează să fie procesate în ordine. Receptorul trebuie să memoreze în buffere datele care au fost recepționate după ce a solicitat retransmisia unui cadru cu erori, pentru că numai acel cadru va fi retransmis.

Toate tipurile de ARQ se bazează pe detectarea erorilor și pe retransmisia datelor care au prezentat erori. Per total, ARQ este cea mai bună variantă pentru corectarea erorilor impuls, deoarece acest tip de distorsiuni apar, în mod normal, într-un procent mic de cadre și nu presupun multe retransmisii. Datorită feedback-ului inherent în protocoalele ARQ, trebuie utilizate linii *semiduplex* sau *duplex complet* întrucât comunicațiile ARQ se produc în ambele sensuri. Dacă sunt disponibile numai legături *simplex*, tehnicile ARQ sunt imposibil de utilizat deoarece receptorul nu va putea să înștiințeze NIC-ul expeditor cu privire la apariția blocurilor de date cu erori.

Fiind o alternativă la ARQ, FEC corectează automat erorile care pot fi remediate la nivelul stratului fizic al NIC-ului receptor, fără a face apel la NIC-ul expeditor. Acest lucru este posibil deoarece NIC-ul expeditor include în transmisie suficienți biți redundanți pentru cazul în care unii dintre aceștia se pierd ca urmare a erorilor. Acest lucru face ca FEC să fie potrivit pentru legăturile de comunicații simplex și pentru cazurile în care nu este realizabilă o cale de întoarcere a semnalelor la NIC-ul expeditor.

De exemplu, să luăm în considerație cazul transmiterii de date fără fir pentru controlul unei sonde spațiale care orbitează în jurul lui Pluto. Între momentul la care NIC-ul expeditor primește înfirmarea de la sondă și momentul la care retransmisia corespunzătoare ajunge la sondă, probabil că aceasta se va prăbuși datorită întârzierii semnificative de propagare. Majoritatea rețelelor fără fir se află pe Pământ, însă întârzierile datorate propagării pot fi totuși suficient de importante pentru a justifica utilizarea FEC.

În ciuda capacității FEC de a corecta erorile fără a face apel la NIC-ul expeditor, ARQ rămâne, totuși, cea mai comună metodă de control al erorilor. Acest lucru se petrece, în primul rând, pentru că erorile apar grupate, de obicei, datorită zgomotului de tip impuls. În acest caz este necesară corectarea unui număr mare de erori, ceea ce, în mod normal, FEC nu poate realiza fără o redundanță excesivă în transmisia datelor.

Însă, multe sisteme de comunicații utilizează, o combinație între ARQ și FEC. În acest caz, dispozitivele din stratul fizic încearcă să corecteze un număr redus de erori pentru a evita retransmisia. Dacă FEC corectează toate erorile, mecanismul ARQ nu va mai trebui să retransmită cadrul de date. Dacă există un număr mare de erori, ARQ intervine, iar expeditorul va retransmite cadrul.

Transferul fără fir al semnalelor purtătoare de date

Mediul aerian nu oferă nici o componentă activă pentru rețeaua fără fir. Câteva elemente pasive afectează însă aspectul și eficacitatea semnalelor pentru transmisia fără fir a informațiilor. De exemplu, în timpul propagării prin mediu, se va produce atenuarea semnalelor, datorită întâlnirii obiectelor solide sau datorită vremii, dar și o pierdere de putere datorată distanței dintre NIC-ul expeditor și cel receptor. În plus, semnalele care se propagă prin mediu pot întâlni interferențe, se pot produce *propagări pe mai multe căi* (care produc distorsiuni) sau alte fenomene care pot afecta semnalele. În capitolul 3 puteți găsi mai multe detalii privitoare la aceste distorsionări ale semnalelor.

Conectarea la infrastructura rețelei fără fir

Stația de bază, cum ar fi un punct de acces, conține atât un NIC fără fir cât și unul cu fir, precum și software-ul care realizează interfețele cu cele două rețele. Atunci când un utilizator fără fir comunică cu un alt utilizator fără fir, stația de bază poate să retransmită, pur și simplu, cadrul de date recepționat de la un utilizator, astfel încât celălalt utilizator să îl poată recepționa. În acest caz, stația de bază se comportă ca un repetor. Dacă destinatarul este localizat undeva în partea cu fir a rețelei, stația de bază va transfera datele prin porțiunea cu fir a rețelei.

După recepționarea unui cadru cu date, NIC-ul fără fir din stația de bază convertește undele radio analogice sau semnalul luminos într-un semnal digital și realizează detectarea erorilor pentru a se asigura că datele din cadrul rezultat nu au erori de biți. Dacă sunt prezente erori, mecanismul de control al erorilor va solicita NIC-ului fără fir expeditor să retransmită cadrul de date. După ce se ocupă de cadrele cu erori, NIC-ul fără fir din stația de bază ori va retransmite cadrele, ori le va transfera în partea cu fir a stației de bază.

În general, NIC-ul cu fir implementează o rețea Ethernet care are interfață directă cu sistemele de întreprindere. De obicei, stația de bază conectează rețeaua fără fir la cea cu fir, la nivelurile stratului fizic și al stratului legătură de date. Unele stații de bază realizează și direcționarea, care este o funcție a stratului rețea.



Atunci când traversează partea cu fir a rețelei, semnalele purtătoare de informații rămân în formă digitală, dar sistemele de tipuri diferite pot converti semnalul digital într-o formă potrivită pentru transmisia prin mediul care este utilizat. Semnalul poate suferi o nouă conversie la forma analogică, dacă este necesară transmisia printr-o altă legătură fără fir (cum ar fi legătura prin satelit) pentru a ajunge la destinație.

Rezumatul capitolului

Rețelele fără fir includ componente care permit realizarea de aplicații mobile și de aplicații portabile. Utilizatorii sunt punctele finale ale rețelei fără fir și utilizează dispozitive de calcul proiectate pentru un anumit tip de aplicație. NIC-urile fără fir și stațiile de bază sunt componentele cheie care comunică prin intermediul mediului aerian. Pentru a asigura roaming-ul în interiorul unei clădiri sau al unui oraș, un sistem de distribuție, cum este o rețea Ethernet, interconectează stațiile de bază și realizează interfața utilizatorilor cu serverele și aplicațiile localizate în rețeaua cu fir.

Modelul de referință cu șapte straturi OSI descrie funcțiile necesare pentru o rețea, dar rețelele fără fir implementează doar funcțiile definite de cele două straturi inferioare — stratul fizic și stratul legătură de date. Aceste funcții cuprind accesul la mediu, controlul erorilor și formarea semnalelor radio și a semnalelor luminoase pentru propagarea prin mediu. Totuși, atunci când se instalează o rețea fără fir, este important să vă asigurați că protocoalele care operează în straturile superioare posedă caracteristicile care le permit să contracareze problemele apărute la nivelul rețelei fără fir.

Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. Care sunt factorii de formă cei mai potriviți pentru NIC-urile fără fir utilizate pentru dispozitivele de calcul fără fir de dimensiuni mici?
2. Care sunt exemplele de fenomene atmosferice care afectează propagarea semnalelor de comunicații fără fir prin mediul aerian?
3. Care este scopul principal al unei stații de bază?
4. Care sunt caracteristicile comune ale unui middleware fără fir?
5. În ce straturi ale modelului de referință OSI operează rețelele fără fir?
6. Prin ce diferă transferul de viteză de transmisie a datelor?
7. Adevărat sau fals: Un dispozitiv de calcul stochează datele în formă analogică.
8. În ce fel de tip de semnal trebuie convertită informația, de către o placă NIC fără fir, înainte de a fi transmisă prin mediul aerian?
9. Care este protocolul uzual pentru accesul la mediu, folosit de rețelele fără fir?
10. Explicați cum realizează ARQ controlul erorilor de transmisie.

Ce veți învăța

După citirea acestui capitol, veți putea: ..

- ✓ să înțelegeți caracteristicile generale ale semnalelor radio și ale semnalelor luminoase care influențează propagarea acestora prin mediul aerian;
- ✓ să înțelegeți modul în care rețelele fără fir transformă reprezentările informațiilor pentru a asigura transmisia prin mediul aerian.



CAPITOLUL 3

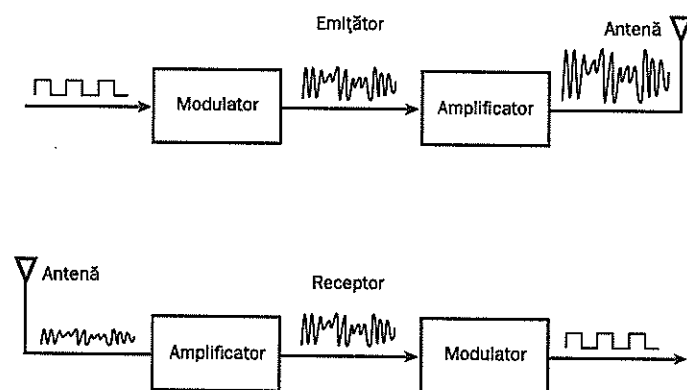
Fundamentele semnalelor de radiofrecvență și ale semnalelor luminoase: mediul invizibil

Diferența fundamentală dintre rețelele fără fir și cele cu fir stă în mediul comunicațiilor. Rețelele cu fir utilizează cablurile pentru a transfera curentul electric care reprezintă informațiile. În cazul rețelelor fără fir, semnalele de radiofrecvență (RF) și semnalele luminoase au sarcina de a transporta informația prin mediul aerian, fără ca acest lucru să fie vizibil. Acest capitol continuă discutarea conceptelor comune tuturor tipurilor de rețele fără fir, punând accent pe fundamentele semnalelor RF și pe fundamentele semnalelor luminoase.

Transceiverele fără fir

Un transceiver fără fir este format dintr-un emițător și un receptor. În emițător, printr-un proces numit *modulare*, sunt convertite semnalele electrice digitale din calculator în semnale RF sau în lumină, care sunt semnale analogice. Apoi, amplificatoarele cresc puterea semnalelor înainte de a fi emise de *antena*. La destinație, un receptor detectează semnalele relativ slabe și le demodulează în tipuri de date utilizabile pentru calculatorul destinatar. Aceste lucruri, care sunt ilustrate de figura 3.1, se petrec în ceea ce se numește un transceiver. Transceiverul este compus, în general, din hardware care constituie o parte a unei plăci de rețea NIC fără fir.

Figura 3.1. În rețelele fără fir, semnalele trec printr-un proces de modulare și de amplificare



Semnalele de radiofrecvență (RF)

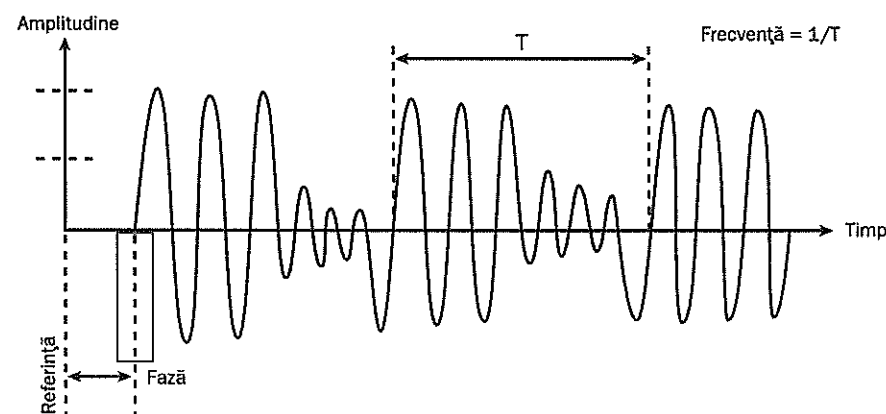
Un *semnal RF* este o undă electromagnetică pe care sistemele de comunicații o folosesc pentru a transporta informațiile prin aer, de la un punct la un altul. Semnalele RF sunt utilizate de multă vreme. Acestea asigură mijloacele de transmisie a muzicii, pentru posturile de radio FM, și a imaginii pentru televiziuni. De fapt, semnalele RF sunt cele mai comune mijloace pentru transportul datelor prin rețelele fără fir.

Caracteristicile semnalelor RF

Semnalele RF se propagă între antenele stațiilor de emisie și de recepție. Așa cum se arată în figura 3.2, semnalul care alimentează antena posedă amplitudine, frecvență și fază. Aceste caracteristici variază în timp pentru a putea reprezenta informațiile.

Amplitudinea indică tăria semnalului RF. În general, măsura amplitudinii este puterea semnalului, care este analoagă cu cantitatea de efort pe care o persoană trebuie să o consume pentru a se deplasa cu bicicleta, pe o anumită distanță. Puterea, în termeni legați de undele electromagnetice, reprezintă cantitatea de energie necesară pentru a „împinge” semnalul pe o anumită distanță. Pe măsură ce puterea semnalului crește, crește și distanța de propagare (raza de acțiune).

Figura 3.2. Amplitudinea, frecvența și faza sunt elementele de bază ale semnalelor RF



Pe măsură ce semnalul radio se propagă prin aer, se produce o scădere a amplitudinii acestuia. Dacă distanța dintre emițător și receptor crește, amplitudinea semnalului scade exponențial cu distanța. Într-un mediu deschis, liber de obstacole, semnalele RF prezintă ceea ce inginerii numesc pierderea în spațiul liber (în limba engleză: free-space loss), care este o formă de atenuare. Atmosfera produce o atenuare exponențială a semnalului modulat pe măsură ce acesta se propagă din ce în ce mai departe față de antenă. Din acest motiv, semnalul trebuie să aibă o putere suficientă pentru a ajunge la distanța dorită la un nivel care să fie acceptabil pentru necesitățile receptorului.

Însă, capacitatea receptorului de a percepe semnalul depinde, de prezența altor semnale RF în vecinătatea sa. Pentru a ilustra acest lucru, imaginați-vă două persoane, Eric și Sierra, aflate la 7 metri una de cealaltă, care încearcă să poarte o conversație. Sierra, în rolul emițătorului, vorbește suficient de tare pentru ca Eric, receptorul, să poată auzi fiecare cuvânt. Dacă bebelușul lor, Madison, țipă mai tare, s-ar putea ca Eric să piardă câteva cuvinte. În acest caz, interferența bebelușului a făcut ca asigurarea comunicațiilor să fie imposibilă. Eric și Sierra trebuie să se apropie unul de celălalt sau Sierra trebuie să vorbească mai tare. Această situație nu diferă prea mult de cea a emițătoarelor și a receptoarelor din sistemele fără fir, care folosesc semnalele RF pentru comunicații.



Frecvența descrie de câte ori pe secundă se produce repetarea semnalului. Unitatea de măsură pentru frecvență se numește Hertz (Hz) și reprezintă numărul de cicluri care se produc într-o secundă. De exemplu, o rețea LAN fără fir 802.11b operează la frecvența de 2,4 GHz, ceea ce înseamnă că semnalul include 2 400 000 000 de cicluri pe secundă.

Faza exprimă cât de mult este decalat semnalul, față de un punct de referință. Prin convenție, fiecare ciclu al semnalului acoperă 360 de grade. De exemplu, un semnal poate avea o diferență de fază (sau o defazare) de 90 de grade, ceea ce înseamnă că decalajul este de un sfert de semnal ($90/360 = 1/4$). O variație de fază este adesea utilă pentru transportarea informației. De exemplu, un semnal poate reprezenta cifra binară 1 la o defazare de 30 de grade și cifra binară 0 la o defazare de 60 de grade. Un avantaj important al reprezentării datelor ca diferențe de fază este acela că distorsiunile rezultate din propagarea semnalului prin mediul aerian nu au mare impact asupra fazelor. În general, distorsiunile afectează amplitudinea, nu faza semnalului.

Pro și contra semnalelor RF

Prin comparație cu semnalele luminoase, semnalele RF au caracteristicile definite în tabelul 3.1.

Tabelul 3.1. Comparație între avantajele și dezavantajele semnalelor RF

Avantajele semnalelor RF	Dezavantajele semnalelor RF
Rază de acțiune relativ mare, până la 30 de kilometri, atunci când nu există obstacole pe direcția de propagare.	Transfer scăzut, până în domeniul Mbps
Operare bună în condiții de ceață, cu excepția situațiilor de ploie torențială, care conduce la performanțe scăzute.	Potențial crescut de producere a interferențelor RF datorate altor sisteme externe bazate pe RF.
Operare liberă de licență (numai pentru sistemele bazate pe 802.11)	Securitate limitată din cauza propagării undelor radio în afara clădirilor.

Argumentele pro determină ca utilizarea semnalelor RF să fie eficientă pentru majoritatea aplicațiilor de rețele fără fir. Majoritatea standardelor pentru rețele fără fir, cum ar fi 802.11 și Bluetooth, specifică folosirea semnalelor RF.

Distorsionarea semnalelor RF

Semnalele RF suferă distorsiuni, datorită interferențelor și a propagării pe mai multe căi. Acest lucru afectează comunicațiile dintre emițător și receptor, producând deseori scăderea performanțelor și nemulțumiri ale utilizatorilor.

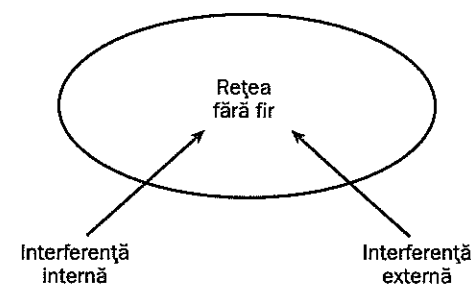
Interferența

Interferența apare atunci când sunt prezente simultan două semnale la stația de recepție, presupunând că acestea au aceeași frecvență și aceeași fază. Această situație este similară cu cea în care o persoană încearcă să asculte alte două persoane care vorbesc în același timp. În această situație, receptoarele NIC-urilor fără fir produc erori atunci când decodifică înțelesul informației care a fost transmisă.

În SUA, Federal Communications Commission (Comisia Federală pentru Comunicații — acronim FCC) reglementează utilizarea majorității benzilor de frecvență și tipurile de modulare pentru a se evita posibilitatea de interferență a semnalelor între sisteme. Însă, interferențele radio pot totuși să apară, mai ales datorită sistemelor care operează pe benzi libere de licență. Utilizatorii sunt liberi să instaleze și să utilizeze echipamente libere de licență, cum sunt LAN-urile fără fir, fără o coordonare a utilizării și a interferențelor.

Figura 3.3 ilustrează forme variate de interferență. Interferența internă se produce atunci când semnale externe interferă cu propagarea semnalelor radio din rețeaua fără fir. Acest tip de interferență poate conduce la apariția de erori în biții de informație care sunt transmiși. Receptorul descoperă, în cele din urmă, erorile, ceea ce conduce la retransmisii și produce întâzieri la utilizatori. Interferențe interne importante pot să apară și dacă un alt sistem radio operează în vecinătate, la aceeași frecvență și utilizând același tip de modulare, cum ar fi cazul a două LAN-uri radio care operează în benzile libere de licență și care sunt apropiate una de cealaltă.

Figura 3.3. Interferențele de semnale radio pot fi interne și externe



Alte surse de interferență internă sunt telefoanele fără fir, cuptoarele cu micro-unde și dispozitivele Bluetooth. Atunci când aceste tipuri de dispozitive RF sunt folosite, performanța unei rețele fără fir poate să se reducă semnificativ datorită retransmisiilor și competiției care apare în rețea pentru utilizarea mediului. Acest lucru solicită o planificare atentă și luarea în considerație a altor dispozitive radio care pot interfera cu rețeaua fără fir.

Una dintre cele mai bune căi de combatere a interferenței RF este eliminarea surselor de interferență. De exemplu, o companie poate stabili o politică prin care să nu fie utilizate telefoanele fără fir care folosesc aceeași bandă de frecvență cu rețeaua fără fir. Însă, problema constă în faptul că este adesea imposibil să se restricționeze complet folosirea unor generatori de interferențe potențiali, cum ar fi dispozitivele Bluetooth. Dacă interferența poate constitui o problemă serioasă, se poate lua în considerație alegerea unei rețele fără fir care să opereze într-o bandă de frecvență care nu se suprapune cu cea a altor dispozitive.

Interferența externă se produce atunci când semnalele de la un sistem de semnale radio interferă cu alte sisteme. Ca și în cazul interferenței interne, interferențe externe importante pot să apară dacă o rețea fără fir se află în vecinătatea unui alt sistem. Deoarece puterea de transmisie a rețelei fără fir este relativ scăzută, interferența externă produce rareori probleme semnificative.

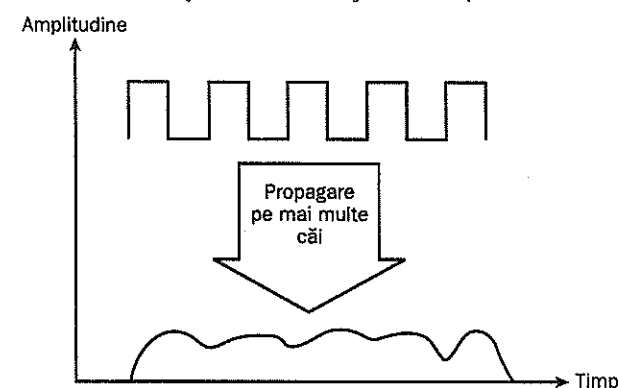
Propagarea pe mai multe căi¹

Propagarea pe mai multe căi se produce atunci când părți dintr-un semnal RF iau căi diferite în propagarea lor de la sursă — cum ar fi o placă NIC radio — la un nod de destinație, cum ar fi un punct de acces (vezi figura 3.4). O parte din semnal poate să meargă direct la destinație; o altă parte se poate reflecta de suprafața unui birou până în tavan și poate ajunge apoi la destinație. Prin urmare, o parte din semnal este întârziat și călătorește pe o cale mai lungă până la receptor.

¹ În limba engleză, multipath propagation (n.tr.).

Întârzierile produse de acest tip de propagare produc distorsiuni ale simbolurilor informațiilor reprezentate în semnalul radio (vezi figura 3.5). Pentru că forma semnalului poartă informațiile care sunt transmise, receptorul va interpreta eronat informațiile din semnal atunci când îl va demodula. Dacă întârzierile sunt destul de mari, apar erori de biți în pachet, mai ales atunci când vitezele de transfer sunt mari. Receptorul nu va putea să distingă simbolurile și să le interpreteze, în mod corect, în biții corespunzători. Atunci când propagarea pe mai multe căi produce astfel de distorsiuni, stația receptoare detectează erorile prin intermediul unui proces de verificare a erorilor. Ca răspuns la erorile de biți, stația emițătoare va retransmite, până la urmă, cadrul de date.

Figura 3.5. Distorsionarea semnalelor datorită propagării pe mai multe căi produce confuzie și erori de biți în receptoare



Datorită retransmisiilor, utilizatorii se confruntă cu performanțe mai scăzute atunci când propagarea pe mai multe căi este semnificativă. De exemplu, semnalele 802.11 din locuințe și birouri pot avea, din acest motiv, întârzieri de 50 de nano-sekunde (ns), în timp ce într-o fabrică pot fi de 300 ns. Pe baza acestor valori, rezultă că propagarea pe mai multe căi nu creează mari probleme în locuințe și birouri. Însă, utilajele și structurile metalice dintr-o fabrică produc o mulțime de suprafețe de reflexie ceea ce produce devieri ale semnalelor RF și căi de transmisie dezordonate. Prin urmare, trebuie să fiți preocupat de problemele create de propagarea pe mai multe căi în depozite, fabrici și în alte locații pline de obstacole metalice neregulate.

Ce puteți face atunci când propagarea pe mai multe căi vă creează probleme? Lăsând la o parte varianta eliminării birourilor și a scaunelor din clădire, diversitatea

pare a fi cea mai bună soluție pentru a combate riscurile legate de propagarea pe mai multe căi. Diversitate înseamnă utilizarea a două antene la fiecare NIC radio pentru a crește probabilitatea de recepționare a unui semnal mai bun printr-una dintre antene.

Antenele pentru diversitate sunt separate fizic pe NIC-ul radio pentru a se asigura că una dintre ele va fi mai puțin afectată de propagări pe mai multe căi decât cealaltă. Cu alte cuvinte, semnalul compus pe care îl recepționează una dintre antene poate fi mai apropiat de cel original decât cel recepționat de cealaltă antenă. Receptorul utilizează software de filtrare a semnalului și de decizie pentru a alege semnalul mai bun pentru demodulare. De fapt, reversul este și el adevărat: emițătorul alege antena mai bună pentru transmisia în direcția opusă.

Semnalele luminoase

Semnalele luminoase au fost folosite în sisteme de comunicații chiar de mai multă vreme decât sistemele RF. Felinarele au constituit o sursă de lumină folosită pentru a transmite coduri între vasele aflate pe mare, cu sute de ani în urmă. Proiectoarele sunt încă în uz astăzi pe multe aeroporturi, ca un sistem de comunicații de rezervă cu avioanele care au defecțiuni la echipamentul radio.

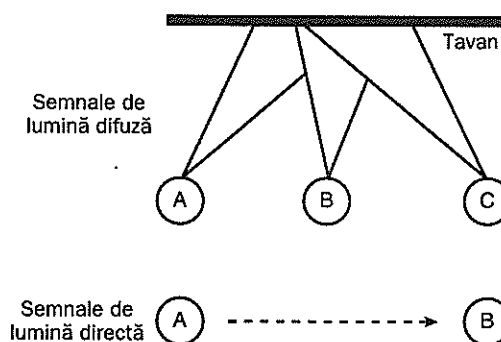
Totuși, rețelele fără fir care utilizează semnalele luminoase nu sunt atât de comune ca acelea care folosesc semnalele radio. În general, semnalele luminoase satisfac cerințele pentru aplicații specializate, cum ar fi legăturile clădire la clădire și rețelele personale pe distanțe scurte. Unele LAN-uri fără fir și unele produse inter-clădiri folosesc lumina laser pentru a transporta informația între calculatoare.

Caracteristicile semnalelor luminoase

Semnalele luminoase au formă analogică și o frecvență foarte înaltă care nu este reglementată de către FCC. Majoritatea rețelelor fără fir care utilizează lumina în scopuri de comunicare fără fir folosesc lumina infraroșie, care are o lungime de undă de aproximativ 900 de nanometri. Această lungime de undă este echivalentă cu o frecvență de 333 333 GHz, care este mult mai mare decât cea a semnalelor RF și care se află imediat sub frecvențele luminii vizibile pentru oameni.

Semnalele infraroșii directe și semnalele infraroșii difuze sunt cele două tipuri principale de transmisie prin lumină. Figura 3.6 ilustrează aceste două concepte. Lumina laser difuză este, de regulă, reflectată de pereți sau de tavan, iar lumina laser directă este focalizată în mod direct, în linie dreaptă, asupra receptorului. Majoritatea LAN-urilor laser utilizează lumina infraroșie difuză; modemurile pentru transmisia între clădiri și PDA-uri folosesc lumină infraroșie directă.

Figura 3.6. Atât semnalele de lumină difuză cât și cele de lumină directă oferă o bază pentru transmisia în rețelele fără fir



Lumina infraroșie are o bandă de frecvență foarte înaltă; însă, tehnica prin difuzie produce o atenuare puternică a semnalului și necesită viteză de transmisie a datelor scăzută (mai mică de 1Mbps) pentru evitarea unor erori semnificative de transmisie. În plus, această tehnică limitează distanța dintre componentele fără fir la aproximativ 13 metri, în principal datorită înălțimii mici a tavanelor încăperilor și a geometriei căii de propagare a semnalului care rezultă din această cauză. Avantajul constă în instalarea relativ ușoară și în componentele ieftine.

Abordarea bazată pe lumina infraroșie directă, numită în mod uzual și optica spațiilor libere, intensifică puterea semnalului luminos în mod similar cu o antenă direcțională pentru semnale radio. Acest lucru crește raza de acțiune a sistemelor laser de putere scăzută până în jurul a 1,5 kilometri, la o viteză de transmisie până la nivelul gigabiților pe secundă.

Ca și în cazul semnalelor RF, amplitudinea semnalelor luminoase scade o dată cu creșterea distanței dintre stația de emisie și cea de recepție. Raza de acțiune a sistemelor cu lumină infraroșie poate varia de la câțiva metri, în cazul aplicațiilor pentru PDA-uri, până la aproximativ 1,5 kilometri în cazul sistemelor cu lumină infraroșie directă. Această rază de acțiune este semnificativ mai mică decât cea a sistemelor RF.



Pro și contra semnalelor luminoase

Prin comparație cu semnalele RF, semnalele luminoase au caracteristicile definite în tabelul 3.2.

Tabelul 3.2. Avantajele și dezavantajele semnalelor luminoase

Avantajele semnalelor luminoase	Dezavantajele semnalelor luminoase
Transfer foarte ridicat, până la nivelul Gbps.	Performanțe variabile și nesigure în prezența smogului, ceții, ploilor și ninsorilor dese sau a unor particule solide în aer.
Protecție a datelor crescută implicit datorită razei laser subțiri.	Rază de acțiune relativ scurtă (1,5 km).
Operare liberă de licență.	Necesitatea operării în linie dreaptă, linie care trebuie să fie liberă de obstacole cum ar fi clădirile, copacii și stâlpii de telefonie.
Potențial extrem de redus de interferență RF cu sisteme externe.	Probleme ridicate de aliniere datorită trepi-dațiilor sau legăturilor clădirilor.

Aceste caracteristici fac ca utilizarea semnalelor luminoase să fie cea mai potrivită pentru aplicațiile specializate la care sunt necesare performanțe extrem de ridicate. De exemplu, o companie poate instala o legătură de comunicații cu lumină infraroșie între două clădiri învecinate pentru a putea asigura efectuarea copiilor de siguranță pentru servere, printr-o rețea fără fir.

Distorsionarea semnalelor luminoase

Propagarea semnalelor de lumină nu este lipsită de probleme. Distorsionările produse de interferențe sau de obstacole limitează performanțele rețelelor fără fir care folosesc semnalele luminoase.

Interferența

Semnalele luminoase nu sunt afectate de sursele RF de interferență, cum sunt telefoanele fără fir și cuptoarele cu microunde. De fapt, FCC nu reglementează utilizarea semnalelor luminoase tocmai datorită potențialului extrem de limitat de interferență între sisteme. Semnalele luminoase au o frecvență atât de înaltă încât emisiile acestora se află mult în afara spectrului sistemelor RF, ceea ce înseamnă că FCC nu reglementează semnalele luminoase.

Însă, interferențele produse de alte surse de lumină pot totuși să constituie o problemă pentru sistemele care utilizează semnalele luminoase. De exemplu, instalarea unui sistem de transmisie punct la punct cu lumină infraroșie, îndreptat pe direcția est-vest, poate conduce la interferențe substanțiale cu lumina infraroșie aflată în emisia solară, atunci când soarele se află puțin deasupra orizontului. În unele cazuri, această interferență poate fi suficient de puternică pentru a întrerupe complet transmisia datelor prin legătura cu lumină infraroșie. Atunci când instalați acest tip de sisteme, asigurați-vă că urmați întocmai recomandările producătorului în momentul orientării antenei.

Atenuarea produsă de obstacole sau de condițiile meteo

Obstacolele, cum ar fi clădirile, munții sau copacii, produc atenuări substanțiale ale semnalelor luminoase pe măsură ce acestea se propagă prin aer. Majoritatea acestor obiecte sunt compuse din materiale care absorb și împrăstie rapid lumina. Prin urmare, trebuie să vă asigurați că respectiva cale dintre punctele finale ale sistemului de comunicații bazat pe lumină este complet liberă de obstacole.

Chiar când calea de comunicații este liberă, vremea poate produce, totuși, atenuări puternice ale semnalelor luminoase. Problema constă în variația condițiilor meteo. De exemplu, o ceață deasă poate fi prezentă, iar apoi cerul poate fi complet senin în orele următoare. Acest lucru determină ca planificarea rezervelor pentru o legătură realizată prin sisteme bazate pe lumină, mai ales pentru acelea care operează către limita razei de acțiune, să fie extrem de dificilă. Planificatorii trebuie să se asigure că atenuarea produsă de vreme nu va întrerupe comunicațiile.

Modularea: pregătirea semnalelor pentru propagare

Modularea produce un semnal radio sau unul luminos care reprezintă datele rețelei într-un mod potrivit pentru propagarea prin aer. Acest lucru implică conversia semnalului digital din calculator într-un semnal analogic. Din acest proces face parte și suprapunerea semnalului purtător de informație peste o purtătoare, care este un semnal ce are o anumită frecvență bine stabilită. De fapt, informația călătorește pe unda purtătoare. Pentru a reprezenta informația, semnalul de modulare modifică purtătoarea de așa natură încât să simbolizeze informația.

Acest lucru este realizat deoarece, în general, nu este practic ca semnalul purtător de informație să fie transmis în forma sa originală. De exemplu, să considerăm că Brian dorește să-și transmită fără fir vocea, de la Dayton la Cincinnati, adică pe o distanță de aproximativ 100 de kilometri. O abordare posibilă pentru Brian ar fi să utilizeze un sistem de amplificare audio de mare putere. Problema este că intensitatea sunetului obținut va produce, probabil, surzirea tuturor locuitorilor din Dayton. În schimb, o abordare mai bună este modularea vocii lui Brian cu un *semnal purtător* de radiofrecvență sau de lumină care se află în afara domeniului frecvențelor auditive și care este adecvat pentru propagarea prin aer. Semnalul de informație poate varia amplitudinea, frecvența sau faza semnalului purtător, iar amplificarea semnalului purtător nu-i va deranja pe oameni deoarece acesta are o frecvență cu mult peste frecvențele auditive.

A doua abordare reprezintă exact ceea ce realizează modularea. Un modulator mixează semnalul sursă de informații, cum ar fi vocea sau datele, cu un semnal purtător. Transceiverul transferă semnalul modulat și amplificat către antenă. Semnalul modulat părăsește antena și se propagă prin aer. Antena stației de recepție transferă semnalul modulat unui demodulator, care separă semnalul de informații de semnalul radio purtător.

Una dintre cele mai simple forme de modulare este modularea în amplitudine, care variază amplitudinea semnalului pentru a reprezenta datele. Acest tip de modulare este comun în sistemele pe bază de lumină în care prezența unui bit 1 „aprinde lumina”, iar prezența unui bit 0 o „stinge”. În realitate, codurile de lumină

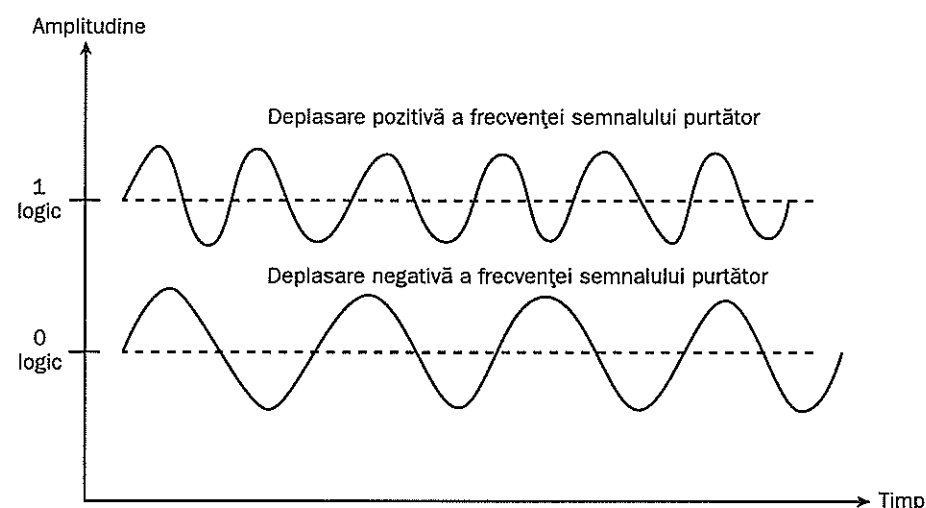
sunt mai complexe, dar ideea de bază este emisia și oprirea emisiei de lumină pentru a transmite datele. Acest lucru este similar cu a oferi niște lanterne unor persoane aflate într-o cameră, în întuneric, pentru a putea comunica prin aprinderea și stingerea repetată a lanternelor care transmit informații codificate.

Pentru sistemele RF, modularea este mai complexă și este descrisă în secțiunile următoare.

Modularea în frecvență (FSK)

Modularea în frecvență (în limba engleză: *frequency shift-keying* — acronim *FSK*) realizează mici modificări ale frecvenței semnalelor purtătoare pentru a reprezenta informațiile într-o formă adecvată pentru propagarea prin aer. De exemplu, așa cum se prezintă în figura 3.7, modularea poate reprezenta biții de date 1 sau 0, fie printr-o variație pozitivă, fie printr-una negativă a frecvenței semnalului purtător. Dacă variația de frecvență este negativă, atunci semnalul purtător se va deplasa către o frecvență mai mică; rezultatul este un 0 logic. Receptorul poate detecta această deplasare în frecvență și poate demodula semnalul ca un bit de date cu valoarea 0.

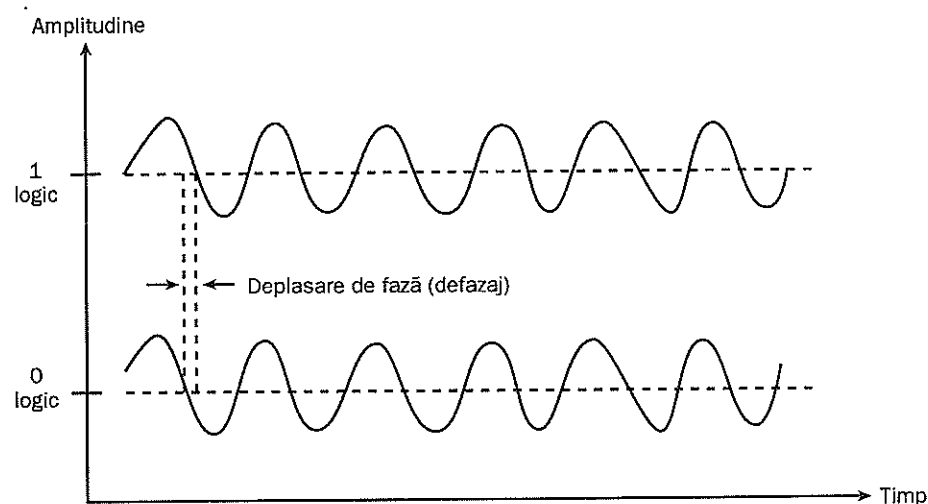
Figura 3.7. FSK utilizează modificările de frecvență pentru a transporta informația



Modularea în fază (PSK)

Similar cu FSK, unele sisteme utilizează *modularea în fază* (în limba engleză: *phase shift-keying* — acronim *PSK*). În cazul utilizării PSK, datele produc modificări ale fazei semnalului purtător, în timp ce frecvența rămâne constantă. Deplasarea de fază, așa cum este reprezentată în figura 3.8, poate corespunde cu o anumită variație pozitivă sau negativă raportată la o referință. Un receptor este capabil să detecteze modificarea de fază și să realizeze corespondența cu biții de date.

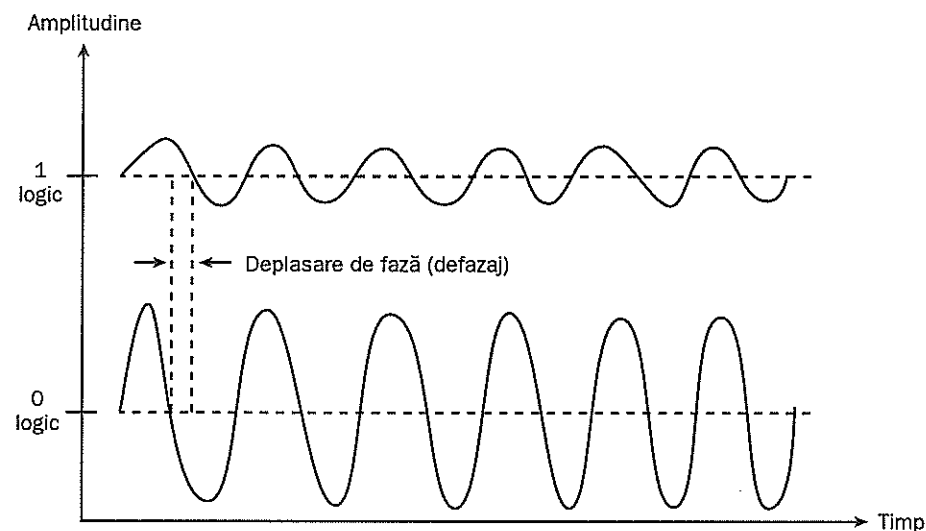
Figura 3.8. PSK utilizează modificările de fază pentru a transporta informația



Modularea în fază și amplitudine (QAM)

Modularea în fază și amplitudine (în limba engleză: *quadrature amplitude modulation* — acronim *QAM*) produce modificări atât ale fazei, cât și ale frecvenței purtătoarei pentru a reprezenta tipare de date, deseori numite simboluri (vezi figura 3.9). Avantajul QAM constă în posibilitatea de a reprezenta grupuri mari de biți printr-o singură combinație amplitudine-fază. De fapt, unele sisteme bazate pe QAM utilizează 64 de combinații diferite amplitudine-fază, ceea ce conduce la reprezentarea a 6 biți de date printr-un simbol. Acest lucru face posibil ca standarde cum sunt 802.11a și 802.11g, să poată asigura viteze de transmisie de date mari.

Figura 3.9. QAM utilizează modificările de amplitudine și de fază pentru a transporta informația



Modularea în spectru larg

În plus față de modularea semnalului digital printr-un semnal analogic purtător folosind FSK, PSK sau QAM, unele rețele fără fir realizează și o dispersare a purtătoarei modulate pe un spectru larg pentru a fi în acord cu reglementările existente. Acest proces, numit *modulare în spectru larg*, reduce în mod semnificativ posibilitatea de producere a interferențelor interne și externe. Prin urmare, în general, corpurile de reglementări nu le solicită utilizatorilor sistemelor cu spectru larg să obțină licențe.

Modularea în spectru larg, dezvoltată inițial pentru aplicații militare, dispersează puterea unui semnal pe o bandă largă de frecvențe (vezi figura 3.10). Componentele pentru spectru radio larg folosesc fie secvența directă, fie salturile de frecvență pentru a dispersa semnalul. Secvența directă modulează o purtătoare radio printr-un cod digital la o viteză de biți mai mare decât lărgimea de bandă a semnalului de informație. Salturile de frecvență presupun salturi rapide ale purtătoarei radio de la o frecvență la alta, toate aflându-se într-un anumit domeniu de frecvențe. Figurile 3.11 și 3.12 ilustrează secvența directă și, respectiv, salturile de frecvență.



Figura 3.10. Spectrul larg ocupă o porțiune largă din spectrul de radiofrecvență

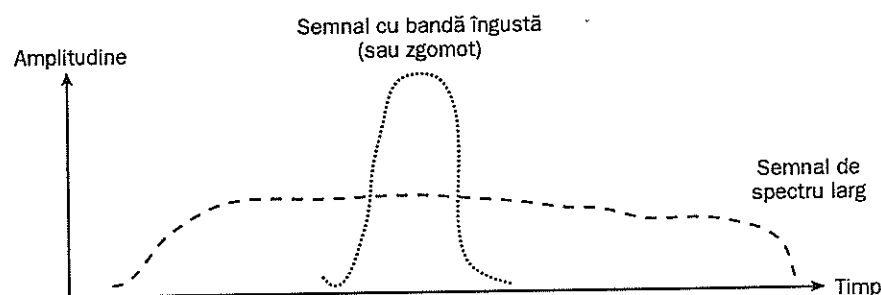


Figura 3.11. Secvența directă este un tip de spectru larg

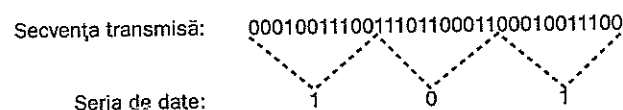
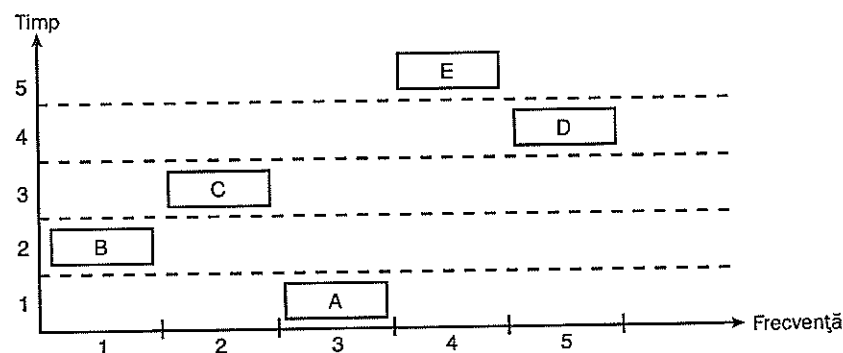


Figura 3.12. Salturile de frecvență sunt un tip de spectru larg



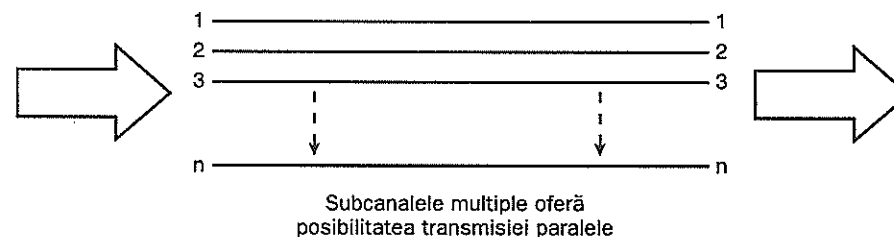
Majoritatea sistemelor cu spectru larg operează în benzile industriale, științifice și medicale (ISM), care au fost autorizate în 1975 de către FCC pentru LAN-urile fără fir. Benzile ISM sunt localizate la 902 MHz, 2,4 GHz și 5,7 GHz. Sistemele RF care operează în bandă ISM trebuie să folosească modularea în spectru larg și să opereze la puteri ale emițătorului de sub 1 watt. Utilizatorii produselor de serie care achiziționează produse care operează în banda ISM nu trebuie să obțină sau să administreze licențe FCC. Acest lucru determină ca instalarea și repoziționarea rețelilor

fără fir să fie ușor de realizat, deoarece problemele legate de administrarea licențelor sunt eliminate. Însă, pentru că benzile ISM sunt deschise pentru public trebuie avută în vedere evitarea interferențelor RF produse ca urmare a funcționării altor dispozitive care operează în aceleași benzi ISM.

Multiplexarea prin divizarea ortogonală a frecvenței

În locul utilizării spectrului larg, unele sisteme fără fir folosesc *multiplexarea prin divizarea ortogonală a frecvenței* (în limba engleză: *Orthogonal Frequency Division Multiplexing* — acronim **OFDM**). OFDM divide semnalul modulat cu FSK, PSK sau QAM pe mai multe semnale purtătoare care ocupă un anumit canal (vezi figura 3.13). OFDM este extrem de eficient, ceea ce permite utilizarea sa pentru a asigura viteze de transmisie a datelor mai mari și pentru a minimiza problemele legate de propagarea pe mai multe căi.

Figura 3.13. OFDM transmite cantități mari de date în paralel, simultan



OFDM a devenit popular pentru transmisii de mare viteză a datelor. În afară de faptul că este specificat de standardele 802.11a și 802.11g pentru LAN-uri fără fir, OFDM stă la baza standardelor europene HiperLAN/2 pentru LAN-uri fără fir. În plus, OFDM este utilizat de ceva vreme pentru a asigura standardul global pentru linia digitală asimetrică de abonat (în limba engleză: *Asymmetric Digital Subscriber Line* — acronim **ADSL**), un standard de telefonie cu fir care realizează o viteză mare de transmisie.

Modularea în bandă ultra-largă

Modularea în bandă ultra-largă (în limba engleză: UWB modulation) a început să câștige teren în fața modulării în spectru larg sau a OFDM, în industria rețelilor fără fir. După ce a fost utilizată pentru o vreme pentru aplicații militare, acum, UWB parcurge procesul necesar pentru autorizarea și dezvoltarea în scopul utilizării publice și comerciale. Chiar dacă pătrunderea UWB a fost întrucâtva lentă, este posibil ca UWB să devină o tehnică superioară pentru multe tipuri de rețele fără fir.

UWB folosește semnale radio în pulsuri scurte de mică putere pentru a transfera datele pe bandă foarte largă de frecvențe. Transmisiile UWB presupun miliarde de pulsuri dispersate pe câțiva gigahertzi. Apoi, receptorul corespunzător traduce pulsurile în date, ascultând secvențele de pulsuri familiare transmise de către emițător.

Inițial, UWB trebuie să asigure lărgimi de bandă cam între 40 și 600 de Mbps, dar, în final, se pot atinge și viteze de transmisie mai mari (la puteri mai mari). De asemenea, sistemele UWB consumă puțină putere, în jur de 1/10 000 din puterea consumată de un telefon celular. Acest lucru face ca UWB să fie practică pentru dispozitive mai mici, cum sunt telefoanele celulare, PDA-urile și chiar ceasurile pe care utilizatorii le pot ține permanent asupra lor.

Deoarece UWB operează la consumuri atât de mici, generează un efect scăzut de interferență cu alte sisteme. UWB produce mai puține interferențe decât sistemele RF convenționale. În plus, spectrul relativ larg utilizat de UWB reduce semnificativ impactul interferențelor cu alte sisteme.

Rămâne însă preocuparea privitoare la interferențe în cazul sistemelor UWB de putere mai mare. FCC plănuiește să reevalueze UWB în viitorul apropiat pentru a studia detaliat chestiunea legată de sistemele de putere mai mare. Până atunci, aveți la dispoziție produse UWB cu distanțe scurte de propagare.

Rezumatul capitolului

Semnalele RF și cele luminoase constituie inima rețelilor fără fir. Acestea oferă un mijloc de transmitere a informației invizibile prin aer. Interferențele generează cele mai periculoase forme de distorsionări de transmisie, care necesită un plan bine gândit atunci când este instalată o rețea fără fir. Tehnici de modulare diverse — FSK, PSK sau QAM — sunt combinate cu spectrul larg sau cu OFDM pentru a se realiza un transceiver, care este un element critic al unei NIC fără fir.

Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. Semnalele RF asigură o rază de acțiune relativ scurtă prin comparație cu semnalele luminoase. Adevărat sau fals?
2. Ce tipuri de condiții meteo afectează cel mai mult semnalele RF?
3. De ce interferențele produc erori în rețelele fără fir?
4. Care sunt sursele interferențelor RF?
5. Propagarea pe căi multiple afectează mai mult sistemele de frecvență 2,4 GHz cu viteze de transmisie a datelor mai mari decât pe cele cu viteze de transmisie a datelor mai mici. Adevărat sau fals?
6. Ce se înțelege prin sistem cu lumină infraroșie difuză?
7. Care este raza de acțiune aproximativă a sistemelor care operează cu lumină infraroșie directă?
8. Ce face modularea astfel încât să fie posibilă transmiterea informațiilor prin aer?
9. Care sunt caracteristicile unui semnal pe care QAM le modifică pentru a realiza reprezentarea informațiilor?
10. În general, spectrul larg necesită licență de utilizator. Adevărat sau fals?

Ce veți învăța

După citirea acestui capitol, veți putea:

- ✓ să recunoașteți tipurile de aplicații PAN fără fir;
- ✓ să înțelegeți componentele PAN-urilor fără fir și standardele utilizate de aceste tipuri de rețele;
- ✓ să înțelegeți bine diversele sisteme PAN fără fir.



CAPITOLUL 4

PAN-uri fără fir: rețele pentru spații restrânse

PAN-urile fără fir satisfac necesitățile de legare în rețea fără fir pentru arii relativ restrânse, cum ar fi între un telefon celular și un laptop. În majoritatea cazurilor, raza de acțiune a PAN-urilor fără fir este de până în 10 metri. Acest lucru face ca PAN-urile fără fir să poată fi utilizate pentru o varietate largă de soluții, însă multe dintre aplicații nu fac decât să înlocuiască cablurile de legătură sau să permită transferuri simple de informații direct de la un utilizator la altul.

Acest capitol definește fiecare dintre componentele primare PAN fără fir, descrie modul de interconectare a acestor componente pentru formarea de sisteme diverse și explorează câteva tehnici radio sau bazate pe lumina infraroșie.

Componente PAN fără fir

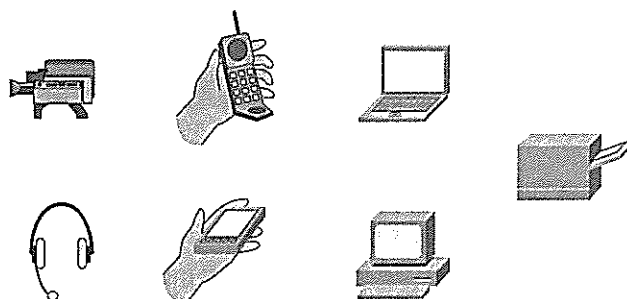
PAN-urile fără fir utilizează atât tehnici radio, cât și tehnici bazate pe lumina infraroșie pe care producătorii le includ în multe tipuri de dispozitive diferite.

Dispozitive pentru utilizator

PAN-urile fără fir nu necesită o putere mare a bateriilor de alimentare pentru a funcționa, ceea ce le face ideale pentru dispozitivele de dimensiuni reduse ale utilizatorilor, cum ar fi aparatele cu căști audio fără fir, telefoanele celulare, PDA-urile, jocurile electronice, unitățile GPS, camerele digitale și laptopurile. Figura 4.1 ilustrează câteva dintre aceste tipuri de dispozitive. De exemplu, o PAN fără fir poate oferi cuiva posibilitatea de a asculta muzica de pe PDA-ul său, printr-un aparat cu căști fără fir. Sau, o persoană poate transfera agenda de telefoane din laptopul său

într-un telefon mobil. În aceste cazuri, PAN-urile fără fir elimină firele care îi deranjează adesea pe utilizatori.

Figura 4.1. Multe tipuri diferite de dispozitive de utilizator funcționează prin intermediul PAN-urilor fără fir



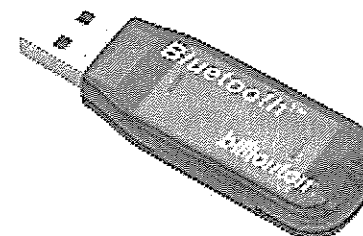
NIC-uri radio

NIC-urile radio sunt disponibile pentru PAN-uri fără fir în formă de placă PC și Compact Flash (CF). Dacă, de exemplu, aveți un laptop este ușor să-i adăugați conectivitate PAN fără fir instalând o placă PC. Aceste produse sunt disponibile la diverși producători. Multe dintre PDA-urile și laptopurile mai noi sunt echipate cu una sau mai multe interfețe PAN fără fir. Acest lucru face ca aceste dispozitive fără fir să fie gata de conectare cu alte dispozitive, cum ar fi imprimantele, PDA-urile și telefoanele celulare care au, și acestea, interfețe PAN fără fir. Plăcile PC de dimensiuni mai mari nu sunt, în mod obișnuit, utilizate pentru PAN-urile fără fir, în primul rând pentru că tehnicile PAN fără fir sunt ideale pentru dispozitivele de dimensiuni mici.

Adaptoare USB

Câteva companii producătoare oferă adaptoare USB pentru PAN-uri fără fir (vezi figura 4.2), care mai sunt numite și chei fără fir (în limba engleză: wireless dongles). De exemplu, puteți achiziționa un adaptor USB Bluetooth și îl puteți conecta la portul USB al PC-ului dumneavoastră. Acest lucru face ca PC-ul dumneavoastră să se poată sincroniza cu alte dispozitive care au conectivitate Bluetooth. Bluetooth — care va fi discutat mai târziu — este o specificație realizată pentru transceivere radio cu rază de acțiune scurtă.

Figura 4.2. Adaptoarele USB fără fir Bluetooth permit ca PC-urile și laptopurile să fie conectate la alte dispozitive Bluetooth



Un PDA care utilizează Bluetooth poate să se conecteze fără fir la un PC care posedă adaptor Bluetooth și se pot sincroniza fără plasarea PDA-ului într-un dispozitiv de sincronizare. Însă, o conexiune USB prin Bluetooth este, în general, mai lentă decât o interfață cu fir realizată direct prin portul USB la PC-ului. Aceasta deoarece adaptorul USB fără fir este mapat la portul serial al PC-ului, care lucrează mai lent decât portul USB. Soluția fără fir poate fi mai convenabilă, dar va trebui să așteptați o perioadă de timp dublă înainte ca sincronizarea să se încheie.

Router

Majoritatea aplicațiilor PAN fără fir presupun numai înlocuirea cablurilor, însă unii producători comercializează routere echipate Bluetooth pentru asigurarea de conexiuni fără fir la Internet. Totuși, datorită razei de acțiune limitate, aceste routere PAN fără fir sunt destinate, în primul rând, utilizării în locuințe și în sediile mici. Pentru a satisface mai multe necesități de conectivitate, unele routere PAN fără fir posedă și interfețe pentru LAN-uri fără fir, cum ar fi 802.11.

Sisteme PAN fără fir

În general, sistemele PAN fără fir se aplică pentru utilizatori individuali, iar unele pot accepta mai mulți utilizatori. Să studiem mai îndeaproape câteva configurații de sisteme PAN fără fir.

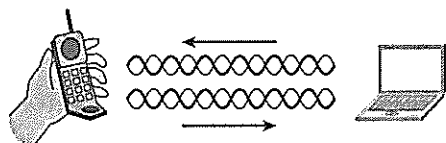
Sisteme pentru locuințe și sedii mici

Există multe configurații diferite pentru sistemele de PAN-uri fără fir din locuințe și din sediile mici.

Sincronizarea

Una dintre cele mai comune utilizări a PAN-urilor fără fir este sincronizarea unui PDA sau a unui telefon celular cu un laptop sau cu un PC. Figura 4.3 ilustrează interconectarea componentelor pentru un astfel de tip de sistem. Atunci când utilizatorul apasă pe butonul „sync” al unui dispozitiv de mână, NIC-ul radio din dispozitivul respectiv transmite datele corespunzătoare către NIC-ul radio al laptopului sau al PC-ului. Tot așa, laptopul sau PC-ul vor transmite date către dispozitivul de mână. În majoritatea cazurilor, conexiunea fără fir extinde portul serial RS-232 la dispozitivul de mână.

Figura 4.3. Sincronizarea transferă informații între două dispozitive, în ambele sensuri



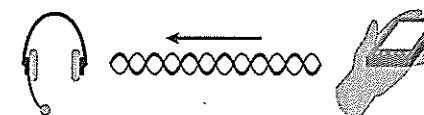
Fluxul continuu de multimedia¹

Un mare număr de aplicații PAN fără fir implică un flux continuu audio sau video. De exemplu, un utilizator poate asculta, cu ușurință, în flux continuu, fișiere MP3 stocate pe un player MP3 (vezi figura 4.4). Multe PDA-uri au posibilitatea de a reda fișiere audio MP3 prin instalarea unuia dintre programele media player populare, cum este media player-ul RealOne de la RealNetworks, Inc. În cazul utilizării unei PAN fără fir, utilizatorul nu mai trebuie să poarte cu el player-ul MP3 și să se încurce în fire sau să stea în aceeași arie restrânsă pentru a asculta muzică. O configurație similară presupune și utilizarea unui set fără fir de casă plus microfon pentru operarea hands-free² a unui telefon celular. Însă, o consecință a acestei abordări este aceea că bateriile se vor consuma mai repede atunci când este utilizată conexiunea fără fir.

¹ În limba engleză, streaming multimedia (n. tr.).

² Mod de folosire a unui telefon celular care lasă mâinile libere pentru alte activități (n. tr.).

Figura 4.4. PAN-urile fără fir permit, cu ușurință, utilizarea unui set de căști plus microfon



Un alt avantaj al utilizării PAN-urilor fără fir în aplicațiile cu flux continuu este conectivitatea flexibilă dintre camerele video și un server. De exemplu, proprietarul unei locuințe poate plasa camere Web în poziții strategice în scopuri legate de monitorizarea pentru securitate. O cameră video ascunsă, îndreptată către zona din fața ușii de la intrare, permite proprietarului să vadă vizitatorii înainte de a le deschide ușa. În acest caz, utilizarea unei conexiuni fără fir simplifică instalarea deoarece elimină necesitatea instalării de cabluri până la camera video. Utilizarea curentului electric sau a bateriilor este în continuare necesară pentru a alimenta camera video, însă prizele electrice sunt disponibile peste tot într-o locuință.

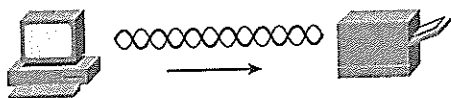
Legătura cu perifericele

PAN-urile fără fir elimină firele pentru periferice, cum ar fi mouse-uri fără fir, tastaturi fără fir, conexiune la telefon fără fir, ceea ce face mai ușoară mutarea și instalarea PC-urilor. Un utilizator poate, de exemplu, să utilizeze o tastatură de dimensiuni normale conectată fără fir la un laptop sau la un PDA. În plus, PAN-urile fără fir reduc încâlceala de cabluri care înconjoară un PC. Fiabilitatea este mai ridicată deoarece sunt mai puține cabluri care s-ar putea defecta și există un risc mai scăzut ca cineva să smulgă, din neatenție, cablurile.

Tipărirea

Legăturile între PC-ul dumneavoastră și imprimantă pot fi realizate, în interiorul unei încăperi, printr-o conexiune PAN fără fir (vezi figura 4.5). Cablurile de imprimantă sunt adesea prea scurte, ceea ce vă obligă să plasați imprimanta într-o locație care nu este cea ideală. Conexiunea PAN fără fir permite mutarea imprimantei într-o poziție mai bună.

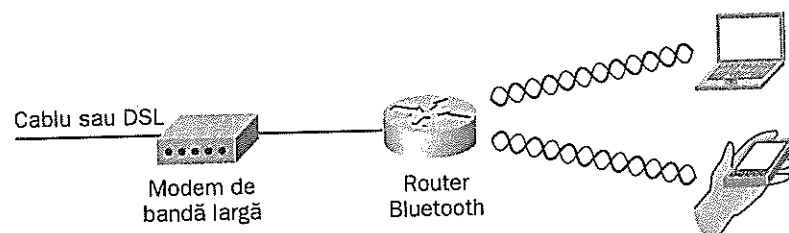
Figura 4.5. Tipărirea este mai ușoară dacă se utilizează o PAN fără fir



Legăturile la Internet

Un utilizator poate accesa e-mail-ul și poate naviga pe Web de oriunde dintr-o cameră prin intermediul unei interfețe PAN fără fir cu Internetul. De exemplu, în loc să stea la un birou, utilizatorul poate sta pe un șezlong sau pe o canapea. Această libertate face ca lucrul cu calculatorul să fie mai plăcut. Figura 4.6 prezintă configurația sistemului care face posibil acest lucru.

Figura 4.6. Un router PAN fără fir asigură conectivitate cu Internetul



Întreprinderi

Utilizarea PAN-urilor fără fir în întreprinderi (în firmele mari) este uzuală; de fapt, aplicațiile și configurațiile sistemelor sunt similare cu cele utilizate în locuințe sau în firmele mici. Angajații folosesc PAN-uri fără fir pentru a sincroniza PDA-uri cu PC-ul de birou și pentru a profita de avantajele oferite de perifericele fără fir. Însă, în loc să utilizeze un router PAN fără fir pentru conectarea utilizatorilor la Internet, o întreprindere folosește o rețea LAN fără fir pentru conectivitatea cu Internetul. Întreprinderile se întind pe suprafețe prea mari pentru ca utilizarea PAN-urilor fără fir să fie practică, aceasta necesitând, în aceste condiții, un număr destul de mare de stații de bază.

Tehnici PAN fără fir

Tehnicile PAN fără fir folosesc atât semnale de radio frecvență cât și lumina infraroșie, în funcție de aplicație.

802.15

Grupul de lucru pentru standardele IEEE 802.15 se concentrează asupra dezvoltării de standarde pentru PAN-uri fără fir și asupra corelării cu alte standarde, cum ar fi standardele 802.11 pentru LAN-uri fără fir.

Grupul de lucru pentru standarde 802.15 cuprinde următoarele elemente:

- **802.15.1** — Grupul de lucru Task Group 1 definește standardele pentru PAN-uri fără fir bazate pe specificațiile Bluetooth versiunea 1.1, care utilizează salturile de frecvență în spectru larg (în limba engleză: frequency hopping spread spectrum — acronim FHSS) și operează cu viteze de transmisie de până la 1 Mbps. Grupul 802.15 a publicat standardele 802.15.1 în iunie 2002, aceste standarde fiind destinate pentru a servi ca resursă pentru producătorii dispozitivelor Bluetooth.
- **802.15.2** — Grupul Task Group 2, responsabil cu acest standard, definește practicile recomandate pentru a facilita coexistența rețelelor 802.15 cu rețelele 802.11. O problemă este cea legată de faptul că ambele tipuri operează în aceeași bandă de frecvență de 2,4 GHz, ceea ce face necesară corelarea funcționării acestor rețele. Grupul cuantifică interferențele și propune metode pentru combaterea acestora.
- **802.15.3** — Grupul Task Group 3 lucrează la un standard nou pentru PAN-uri fără fir cu viteze mai mari de transmisie. Vitezele de transmisie avute în vedere sunt de 11, 22, 33, 44 și 55 Mbps. Combinate cu vitezele de transmisie mai mari, mecanismele de calitate a serviciilor (QoS) fac ca acest standard să fie bun pentru a satisface necesitățile aplicațiilor multimedia. Acest grup își îndreaptă atenția și asupra cerințelor de scădere a costurilor și a puterilor consumate. Un proiect al standardului 802.15.3 este acum disponibil pentru achiziționare.
- **802.15.4** — Grupul Task Group 4 investighează definirea unui standard ce presupune viteze de transmisie a datelor scăzute dar care conduc la consumuri foarte scăzute de putere pentru dispozitivele mici la care înlocuirea bateriilor



nu e practică decât la intervale de ordinul lunilor sau anilor. De exemplu, candidați pentru această tehnică sunt: senzorii, insignele inteligente și sistemele de automatizare casnice. Vitezele de transmisie avute în vedere sunt de 20, 40 și 250 Kbps. Un proiect al standardului 802.15.4 este acum disponibil pentru achiziționare.



Notă

Mai multe informații referitoare la standardul 802.15 puteți găsi la <http://grouper.ieee.org/groups/802/15/>.

Bluetooth

Introducerea în 1998 a specificației Bluetooth a fost rezultatul cooperării a mai multor companii (Ericson, IBM, Intel, Nokia și Toshiba) pentru crearea unei soluții în problema accesului fără fir între dispozitive de calcul. Bluetooth, care este o specificație, nu un standard, este ideal pentru dispozitive de mici dimensiuni, cu raze scurte de acțiune, consumuri scăzute și legături radio ieftine. Acest lucru face ca Bluetooth să fie o soluție bună pentru conectarea dispozitivelor de dimensiuni mici din raza de acțiune a unei persoane aflate într-o arie de lucru restrânsă. Acesta este motivul pentru care grupul 802.15 a ales Bluetooth ca bază a standardului 802.15.1.

Caracteristicile de bază

Special Interest Group (SIG — Grupul de Interese Speciale) a publicat versiunea inițială a specificației Bluetooth la mijlocul anului 1999. De atunci au fost făcute mai multe actualizări, însă caracteristicile tehnice sunt esențialmente aceleași. Transceiverele Bluetooth funcționează până la viteze de transfer al datelor de 1 Mbps, în banda de frecvență de 2,4 GHz, folosind tehnica FHSS. Se realizează salturi de frecvență pe întreg spectrul, cu o periodicitate de 1600 de salturi pe secundă, ceea ce este mai rapid decât în cazul versiunii 802.11 a salturilor de frecvență.

Dispozitivele Bluetooth de putere scăzută au o rază de acțiune de 10 metri. Dispozitivele Bluetooth cu o putere mai mare pot ajunge până la distanțe de aproximativ 100 de metri. Varianta de putere mare este, totuși, rar folosită.

Modulele Bluetooth au factori de formă relativ mici. Dimensiunile tipice sunt de 10,2 x 14 x 1,6 mm, ceea ce este suficient de puțin pentru a se putea potrivi la o varietate de dispozitive de utilizator.

Bluetooth asigură conectarea automată între dispozitivele Bluetooth care se află în raza comună de acțiune, însă utilizatorul are posibilitatea de a accepta sau de a respinge conexiunile cu anumiți utilizatori. Însă, utilizatorii vor trebui întotdeauna să știe dacă conexiunea lor Bluetooth este permisă. Pentru a asigura securitatea, conexiunea Bluetooth va fi dezactivată. Specificația prevede și posibilitatea criptării.

Va putea Bluetooth să înlocuiască LAN-urile fără fir?

Bluetooth are caracteristici asemănătoare cu LAN-urile fără fir. Prin folosirea versiunii Bluetooth de putere mare, producătorii pot realiza puncte de acces Bluetooth și routere Bluetooth cu raze de acțiune similare cu rețelele 802.11. Însă, produsele Bluetooth obișnuite sunt, în general, de putere mai redusă și sunt dedicate funcțiilor PAN fără fir. În plus, va fi dificil pentru produsele LAN-urilor fără fir Bluetooth să pătrundă pe piață, deoarece produsele 802.11 sunt deja adoptate pe scară largă.

Bluetooth se află în urma 802.11 din punctul de vedere al performanțelor și al razei de acțiune. Componentele 802.11 pot atinge viteze de transmisie de până la 54 Mbps, în vreme ce Bluetooth se află în urmă, în jurul valorii de 1 Mbps. Această valoare poate fi suficientă pentru cele mai multe aplicații de înlocuire de cablu — cum ar fi o interfață între un set cască plus microfon și un PDA — însă sunt necesare performanțe mai ridicate pentru a naviga pe Web printr-o conexiune de bandă largă sau pentru a face parte dintr-o rețea de întreprindere. De asemenea, raza de acțiune obișnuită a lui 802.11 este de 100 de metri în interiorul clădirilor, ceea ce este mult mai mult decât poate asigura Bluetooth. În cazul utilizării Bluetooth vor fi necesare mai multe puncte de acces pentru a acoperi complet zone mai mari.

Prin urmare, este puțin probabil ca produsele Bluetooth să câștige în fața celor 802.11. Acest lucru este evident, fără îndoială, pentru că magazinele de electronice vând, în primul rând, produse (Wi-Fi) 802.11 pentru aplicațiile LAN fără fir și nu produse Bluetooth.

Vor putea LAN-urile fără fir să înlocuiască Bluetooth?

Este posibil ca LAN-urile fără fir 802.11 să aibă un impact puternic asupra vânzărilor de dispozitive Bluetooth, mai ales pentru că produsele 802.11 ating sau depășesc aproape toate caracteristicile produselor Bluetooth. Datorită faptului că adoptarea pe scară largă a produselor Bluetooth nu s-a produs încă, există posibilitatea ca aceia care comercializează componentele 802.11 să pună piedici producătorilor care au nevoie de sprijin pentru produsele PAN fără fir.



Totuși, ar trebui făcute unele modificări. Dimensiunile componentelor 802.11 trebuie să devină mai mici, însă acest lucru începe să devină o realitate, pe măsură ce companiile producătoare de materiale semiconductoare fac tot posibilul ca să miniaturizeze seturile de cipuri 802.11. Aceste componente de dimensiuni mai reduse necesită un consum de putere mai scăzut, ceea ce le face mai competitive pentru dispozitivele, cum ar fi telefoanele mobile, care posedă baterii mai mici. În situația în care grupul 802.15 definește standardele pentru PAN-urile fără fir bazate pe Bluetooth — iar grupul 802.11 se concentrează asupra LAN-urilor fără fir — este probabil că Bluetooth și 802.11 vor continua să coexiste și să fie complementare.

Minimizarea interferențelor Bluetooth

Pe măsură ce devin disponibile mai multe produse fără fir, va trebui să vă ocupați cu atenție de interferențele potențiale de frecvențe. Testele au evidențiat interferențe semnificative între Bluetooth și alte sisteme care funcționează în banda de 2,4 GHz, cum sunt LAN-urile fără fir 802.11. O problemă critică este legată de faptul că Bluetooth și 802.11b nu se înțeleg reciproc și nici nu urmează aceleași reguli. Un sistem Bluetooth radio poate începe întâmplător o transmisie de date în timp ce o stație 802.11 transmite un cadru. Acest lucru conduce la producerea unei coliziuni, ceea ce forțează stația 802.11 să retransmită cadrul. Această lipsă de coordonare constituie sursa interferențelor de radio frecvență (RF) dintre Bluetooth și 802.11.

Datorită potențialului de apariție a coliziunilor, rețelele 802.11 și cele Bluetooth prezintă performanțe reduse. O stație 802.11 își micșorează automat viteza de transmisie a datelor și retransmite cadrele atunci când apar coliziuni. În consecință, protocolul 802.11 introduce întârzieri în prezența interferențelor cu sistemele Bluetooth.

Influența completă a interferențelor RF depinde de modul de utilizare și de apropierea de dispozitivele Bluetooth. Interferențele apar numai atunci când dispozitivele Bluetooth și 802.11b transmit în același timp. Utilizatorii pot avea dispozitive Bluetooth în laptopurile sau PDA-urile lor, însă interferențele nu vor exista dacă aplicațiile nu utilizează semnalele radio Bluetooth pentru transmiterea de date.

Unele aplicații Bluetooth, cum ar fi tipărirea de pe un laptop sau sincronizarea unui PDA cu un PC, folosesc semnalele radio pentru o scurtă perioadă de timp. În acest caz, dispozitivele Bluetooth nu sunt active destul de mult timp pentru a afecta semnificativ performanța rețelei 802.11. De exemplu, un utilizator poate să-și sincronizeze PDA-ul cu PC-ul atunci când sosește la serviciu, dimineața. În afară de acest moment, dispozitivul radio Bluetooth poate fi inactiv și în felul acesta nu va produce interferențe în restul zilei.

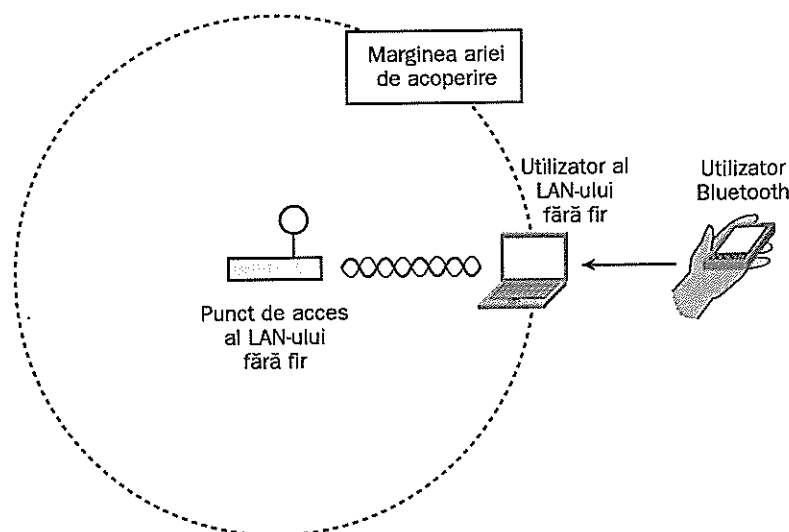
Cel mai mare impact se produce atunci când o companie implementează pe scară largă o rețea Bluetooth, cum ar fi una care asigură mobilitatea pentru medicii și asistentele medicale care utilizează PDA-urile într-un spital. Dacă rețeaua Bluetooth acoperă o arie largă și este utilizată la nivel moderat către înalt, atunci e probabil că sistemul Bluetooth va produce un număr substanțial de coliziuni cu semnalele rețelei 802.11 aflate în aceeași zonă. În acest caz, Bluetooth și 802.11 vor avea dificultăți în a coexista, iar performanțele probabil că vor avea de suferit.

În afară de modul de utilizare, apropierea dispozitivelor Bluetooth față de NIC-urile radio 802.11 și față de punctele de acces are un efect foarte important asupra gradului de interferență. Puterea de transmisie a dispozitivelor Bluetooth este, în general, mai scăzută decât cea a LAN-urilor fără fir 802.11. De aceea, o stație 802.11 trebuie să fie relativ aproape (în jur de 3 metri) de un dispozitiv Bluetooth care transmite pentru ca să se producă o interferență semnificativă.

O aplicație tipică, care se potrivește cu acest scenariu, este cea în care un utilizator de laptop folosește Bluetooth pentru a asigura conexiuni cu un PDA și cu o imprimantă precum și standardul 802.11 pentru a accesa Internetul și serverele de corporație. În această situație, potențialul de producere a interferențelor este enorm, mai ales atunci când utilizatorul operează la limita ariei de acoperire a rețelei 802.11. Figura 4.7 ilustrează această situație. Probabil că semnalul de la dispozitivul Bluetooth va acoperi semnalul 802.11 care este atenuat datorită distanței mari față de punctul de acces.



Figura 4.7. Interferențele RF pot să apară între transmisiile dispozitivelor Bluetooth și cele ale LAN-ului fără fir 802.11



Iată câteva sfaturi privitoare la modul în care pot fi evitate interferențele pornite de la dispozitivele Bluetooth:

- **Managementul utilizării dispozitivelor RF** — O cale de reducere a potențialului de producere a interferențelor constă în reglementarea tipurilor de dispozitive RF utilizate în locuința sau în sediul firmei dumneavoastră. Cu alte cuvinte, stabilirea unui regulament intern privitor la folosirea dispozitivelor RF fără licență. Măsura extremă constă în interzicerea completă a utilizării Bluetooth; însă, acest lucru nu e practic, iar în unele cazuri chiar nu e posibil. De exemplu, nu este realizabilă interzicerea folosirii Bluetooth în zonele publice sau în sediile mari. Pentru aplicații private, puteți stabili reguli interne de companie pentru limitarea utilizării Bluetooth la anumite aplicații, cum ar fi sincronizarea PDA-urilor cu PC-urile.
- **Asigurarea unei acoperiri 802.11 adecvate** — Semnalele 802.11 puternice în interiorul zonei de acoperire reduc impactul semnalelor Bluetooth. Dacă transmisiile LAN fără fir devin prea slabe, interferența cu semnalele Bluetooth va crea mai multe probleme. Realizați o examinare amănunțită a zonei din punctul de vedere al semnalelor RF și determinați locația cea mai potrivită pentru punctele de acces.

- **Trecerea la banda de frecvențe de 5 MHz** — Dacă nici unul dintre pașii precedenți nu rezolvă problema, trebuie avută în vedere utilizarea unui tip de LAN fără fir de 5 MHz, cum este 802.11a. Lucrând în această bandă puteți evita complet interferențele — cel puțin în viitorul previzibil.



Notă

Dacă doriți să aflați mai multe despre specificația Bluetooth și despre produsele aferente puteți accesa <http://www.bluetooth.com>.

IrDA

Principalul concurent al Bluetooth este *Infrared Data Association (IrDA)*, care a fost definit și publicat în 1993. IrDa are o cartă pentru crearea unui standard de comunicații seriale de date interoperabile, ieftin, cu consum de putere redus, pentru aplicații pe distanță scurtă. IrDA există de mai multă vreme decât Bluetooth. De fapt, multe laptopuri și telefoane celulare sunt echipate, de mai multă vreme, cu o interfață IrDA.

Caracteristicile de bază

IrDA se bazează pe lumina infraroșie, care nu se transmite prin pereți sau prin alte obstacole. Acest lucru limitează strict raza de acțiune a dispozitivelor IrDA la o încăpere în care nu există obstacole. De aceea, IrDA este util numai pentru aplicațiile punct la punct, cum ar fi sincronizarea PDA-urilor cu PC-urile. Însă, un avantaj al utilizării IrDA este acela că nu trebuie să existe o preocupare pentru interferențele RF.

Standardul de date IrDA, care este cel mai potrivit pentru dispozitive cum ar fi un player MP3 care trebuie să realizeze un flux continuu de informații, asigură o viteză de transmisie a datelor de până la 4 Mbps. Această versiune a standardului are o rază de acțiune de până la un metru, însă versiunile de putere scăzută conservă în mod semnificativ puterea bateriilor și reduce distanța de operare la aproximativ 20 de centimetri.

Pentru a asigura o legătură fără fir eficace cu perifericele unui calculator, cum ar fi o tastatură sau un mouse, versiunea respectivă a standardului (IrDA control version) reduce viteza de transfer a datelor la 75 Kbps. În plus, calculatorul gazdă poate comunica simultan cu până la opt periferice.

**Notă**

Dacă doriți să aflați mai multe informații despre IrDA și despre produsele aferente puteți accesa <http://www.irda.org>.

Rezumatul capitolului

PAN-urile fără fir sunt destinate să asigure conexiuni de rețea fără fir pe arii restrânse, cum ar fi în interiorul unei încăperi. Dispozitivele echipate cu Bluetooth sau IrDA reduc în mod semnificativ numărul de cabluri folosite, ceea ce conduce la flexibilitatea aplicațiilor — cum ar fi funcționarea hands-free a telefoanelor celulare, ascultarea muzicii la playere audio cu flux continuu sau sincronizarea unui PDA cu un PC. Multe dintre tipurile de aplicații sunt potrivite atât pentru acasă cât și pentru corporații.

Bluetooth și IrDA sunt principalele tehnici pe care le implementează PAN-urile fără fir. Grupul 802.15 a ales să folosească Bluetooth ca bază pentru standardul pentru PAN-uri fără fir 802.15.1. Datorită performanței și razei de acțiune limitate ale Bluetooth nu este probabil ca PAN-urile fără fir să înlocuiască, în viitor, LAN-urile fără fir 802.11.

Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. Care sunt factorii de formă obișnuiți ai plăcilor radio pentru PAN-uri fără fir?
2. Care sunt aplicațiile care pot obține avantaje importante de pe urma utilizării unui adaptor USB fără fir (numit și cheie fără fir)?
3. Când are sens să fie utilizate routerele PAN fără fir?
4. Care este aria de acoperire maximă obișnuită a PAN-urilor fără fir?
5. Care este grupul de standarde IEEE care utilizează specificația Bluetooth ca bază pentru standardul respectiv?
6. În ce bandă de frecvență operează Bluetooth?
7. Care este principala problemă ridicată de funcționarea Bluetooth în apropierea LAN-urilor fără fir 802.11?
8. Un dispozitiv care are capabilitate Bluetooth transmite în permanență. Adevărat sau fals?
9. Care este viteza de transmisie a datelor cea mai ridicată posibilă pentru un dispozitiv IrDA?
10. Care este avantajul utilizării IrDA prin comparație cu Bluetooth?

Ce veți învăța

După citirea acestui capitol, veți putea:

- ✓ să recunoașteți aplicațiile specifice ale LAN-urilor fără fir;
- ✓ să înțelegeți componentele LAN-urilor fără fir și standardele utilizate de aceste tipuri de rețele;
- ✓ să înțelegeți configurarea sistemelor LAN fără fir.



CAPITOLUL 5

LAN-urile fără fir: rețele pentru clădiri și complexe de clădiri

LAN-urile fără fir satisfac, în mod eficient, necesitățile de conectare pentru spații cum ar fi clădirile sau complexe de clădiri. Având performanțe și posibilități de protecție comparabile cu cele ale rețelilor cu fir, soluțiile LAN fără fir se regăsesc în locuințe, sedii de firme mici, întreprinderi mari și în spațiile publice. LAN-urile fără fir pot realiza multe tipuri de aplicații diferite.

Acest capitol definește fiecare dintre componentele principale ale unei rețele LAN fără fir, descrie modul în care sunt interconectate aceste componente pentru a forma o varietate de sisteme și studiază standardele 802.11.

Componente LAN fără fir

LAN-urile fără fir sunt formate din componente similare cu cele ale LAN-urilor cu fir Ethernet tradiționale. De fapt, protocoalele LAN fără fir sunt similare cu cele Ethernet și respectă aceiași factori de formă. Marea diferență constă în faptul că LAN-urile fără fir nu necesită utilizarea de fire (cabluri).

Dispozitive pentru utilizator

Utilizatorii LAN-urilor fără fir lucrează cu o multitudine de dispozitive cum ar fi PC-urile, laptopurile și PDA-urile. Utilizarea LAN-urilor fără fir pentru legarea în rețea a PC-urilor staționare este avantajoasă deoarece limitează necesitatea utilizării cablurilor. Laptopurile și PDA-urile sunt oricum echipate, în mod obișnuit, pentru conectivitate LAN fără fir, datorită naturii portabile a acestora. Dispozitivele pentru utilizatori pot consta și din hardware specializat. De exemplu, scanerele pentru coduri de bare și dispozitivele pentru monitorizarea pacienților posedă adesea conectivitate LAN fără fir.

NIC-uri radio

O componentă importantă a unei LAN fără fir este NIC-ul radio care funcționează într-un dispozitiv de calcul asigurând conectivitatea fără fir. Un NIC radio pentru LAN-uri fără fir, numit uneori și placă radio, implementează deseori standardul 802.11. În general, plăcile implementează un anumit strat fizic, cum ar fi 802.11a sau 802.11b/g. Prin urmare, placa radio trebuie să folosească o versiune a standardului care este compatibilă cu respectiva LAN fără fir. Plăcile radio pentru LAN-uri fără fir, care implementează mai multe versiuni ale standardului și care asigură o mai bună *interoperabilitate*, devin din ce în ce mai comune.

Plăcile radio sunt realizate într-o varietate de factori de formă incluzând: ISA, PCI, placă PC, mini-PCI și CF. În general, PC-urile utilizează plăci ISA sau PCI, însă PDA-urile și laptopurile folosesc plăci PC, mini-PC sau adaptoare CF.

Puncte de acces

Un punct de acces conține o placă radio care comunică cu dispozitivele individuale de utilizator prin intermediul LAN-ului fără fir și o rețea NIC cu fir care realizează interfața cu un *sistem de distribuție*, cum ar fi o rețea Ethernet. Software-ul de sistem din punctul de acces realizează legătura dintre LAN-ul fără fir și partea de sistem de distribuție a punctului de acces. Software-ul de sistem diferențiază punctele de acces prin gradări variate ale funcțiilor de management, instalare și securitate. Figura 5.1 prezintă un exemplu de hardware pentru un punct de acces.

Figura 5.1. Punctele de acces pentru LAN-uri fără fir conectează LAN-urile fără fir la rețelele cu fir (fotografie reprodusă prin amabilitatea Linksys)



În majoritatea cazurilor, punctul de acces oferă o interfață http care permite modificări de configurație a punctului de acces prin intermediul unui dispozitiv de utilizator final care este echipat cu o interfață de rețea și un browser Web. Unele puncte de acces au și o interfață serială RS-232 pentru configurarea punctului de acces printr-un cablu serial și prin intermediul unui dispozitiv de utilizator care rulează emularea de terminal și software-ul Telnet, cum ar fi, de exemplu, hyper terminal.

Configurarea unui punct de acces

Să vedem care sunt setările unei configurări radio de bază pentru un punct de acces Cisco 350. Aceste tipuri de setări sunt comune și pentru alte modele de puncte de acces.

Un parametru care trebuie stabilit este identificatorul setului de servicii (în limba engleză: service set identifier — acronim SSID). SSID furnizează un nume pentru o anumită LAN fără fir pe care utilizatorii îl vor asocia cu aceasta. Pentru motive legate de securitate este bine să stabiliți pentru SSID un nume diferit de cel prestabilit.

Pentru majoritatea aplicațiilor, veți stabili puterea de transmisie a punctului de acces la valoarea maximă, care este, în mod obișnuit, de 100 miliwați, în SUA. Acest lucru va maximiza raza de acțiune a LAN-ului fără fir. Puterea maximă efectivă la ieșire este de 1 watt, dar o putere de transmisie mai scăzută asigură o toleranță suficientă ce permite utilizarea unei antene de mare câștig¹ în condițiile în care transmisia rămâne, în continuare, în limitele stabilite.

În SUA, se stabilește funcționarea punctului de acces pe oricare dintre canalele de la 1 la 11. Atunci când instalați numai un singur punct de acces, nu are importanță ce canal alegeți. Dacă instalați mai multe puncte de acces, sau dacă știți că există o altă LAN fără fir în vecinătatea rețelei dumneavoastră, va trebui să selectați canale diferite, care nu se suprapun (cum ar fi canalele 1, 6 și 11), pentru fiecare dintre punctele de acces care se află în raza de acțiune a altui punct.

Ca o măsură minimală de securitate, activați criptarea WEP (în limba engleză: wired equivalent privacy). Va trebui să stabiliți o cheie de criptare de care vor avea nevoie toate dispozitivele de utilizator pentru a stabili conexiunea cu punctul de acces respectiv. Dacă alegeți să utilizați chei de 40 de biți, introduceți 10 caractere hexazecimale, fiecare dintre acestea fiind o cifră de la 1 la 9 sau o literă de la A la F. Cheile de 104 biți necesită introducerea a 26 de caractere hexazecimale. Rețineți că pentru cheile de 40 de biți corespunde o criptare de 64 de biți, iar pentru cheile de 104 biți corespunde o criptare de 128 de biți, peste cei 24 de biți ai vectorului de inițializare utilizat în ambele cazuri.

¹ Mărime care constituie o măsură a amplificării semnalului de către o antenă (n. tr.).

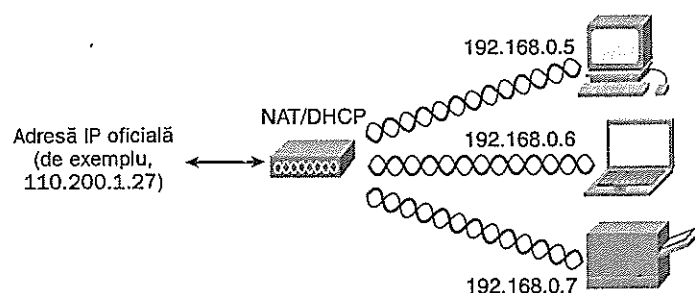
Routere

Prin definiție, un router transferă pachete de date între rețele. Routerul alege legătura următoare cea mai bună pentru a transmite pachete astfel încât acestea să se apropie de destinație. Routerele folosesc antetele IP (în limba engleză: Internet Protocol) ale pachetelor și tabelele de direcționare, precum și protocoalele interne, pentru a determina ruta cea mai bună pentru fiecare pachet.

Un router LAN fără fir adaugă o funcție încorporată de punct de acces la un router Ethernet multiport. Acest lucru combină mai multe rețele Ethernet cu conexiuni fără fir. Un router LAN fără fir tipic include patru porturi Ethernet, un punct de acces 802.11 și, uneori, un port paralel, astfel încât să poată fi un server de tipărire. Lucrul acesta le oferă utilizatorilor conectați fără fir aceleași capabilități pe care le au și utilizatorii conectați cu fir, de a transmite și de a recepționa pachete prin multiple rețele interconectate.

Routerele implementează protocolul pentru *traducerea adreselor de rețea* (în limba engleză: *Network Address Translation* — acronim *NAT*) care permite mai multor dispozitive din rețea să partajeze o singură *adresă IP* oferită de un furnizor de servicii Internet (ISP). Figura 5.2 ilustrează acest concept. De asemenea, routerele implementează serviciile *protocolului pentru configurarea dinamică a gazdelor* (în limba engleză: *Dynamic Host Configuration Protocol* — acronim *DHCP*) pentru toate dispozitivele. DHCP atribuie dispozitivelor adrese IP private (confidențiale). Împreună, NAT și DHCP fac posibil ca un număr de dispozitive de rețea, de pildă PC-uri, laptopuri și imprimante, să partajeze o adresă IP comună de Internet.

Figura 5.2. NAT și DHCP sunt protocoalele esențiale implementate de către routere



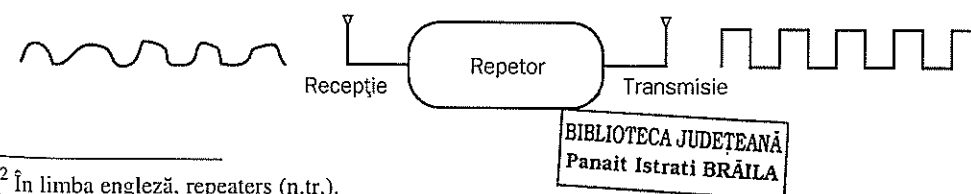
Routerele LAN fără fir oferă avantaje importante în cazul instalării în locuințe sau în sedii de firme mici. De exemplu, vă puteți abona la un serviciu de modem de cablu care oferă unui router o singură adresă IP prin intermediul DHCP, iar routerul furnizează apoi adrese IP, pe baza DHCP, pentru clienții din rețeaua dumneavoastră locală. Apoi NAT mapează un anumit client din rețeaua locală la adresa IP atribuită de ISP, atunci când acest client vrea să acceseze Internetul. Prin urmare, aveți nevoie de un router dacă plănuți să aveți mai multe componente de rețea, în rețeaua locală, care să partajeze o singură adresă IP atribuită de ISP. În loc să aveți un hardware separat pentru router și unul pentru punctul de acces, un router LAN fără fir asigură ambele funcții cu un singur hardware. Însă, routerele sunt rareori utilizate în rețelele mari, cum ar fi cele din spitale sau din sediile centrale de companii. În aceste cazuri, punctele de acces sunt cele mai bune, deoarece rețeaua posedă deja componente conectate prin fir care se ocupă de adresele IP.

Repetoare²

Punctele de acces, care necesită cabluri pentru interconectare, joacă, în general, un rol dominant în asigurarea acoperirii pentru majoritatea LAN-urilor fără fir. Însă, *repetoarele* fără fir constituie o cale de extindere a ariei de acoperire a unei LAN fără fir existente, în locul adăugării de noi puncte de acces. Există puține tipuri de repetoare de sine stătătoare pe piață, însă unele puncte de acces au încorporată funcția de repetor.

Un repetor regenerează, pur și simplu, un semnal de rețea pentru a extinde aria de acoperire a unei infrastructuri existente de rețea (vezi figura 5.3). Un repetor LAN fără fir nu este conectat fizic, prin fir, la nici o parte a rețelei. În schimb, acesta recepționează semnalele radio primite de la un punct de acces, de la un dispozitiv al unui utilizator final sau de la alt repetor și apoi retransmite cadrele. Acest lucru face posibil ca un repetor, care e poziționat între un punct de acces și un utilizator îndepărtat, să acționeze ca un releu pentru cadrele care sunt transferate, în ambele sensuri, între utilizator și punctul de acces.

Figura 5.3. Repetorele LAN fără fir sunt dispozitive simple care nu necesită cabluri



² În limba engleză, repeaters (n.tr.).

Prin urmare, repetoarele fără fir sunt o soluție eficace de contracarare a distorsiunii semnalelor (cum este cea produsă de atenuarea RF). De exemplu, repetoarele asigură conectivitatea pentru zonele îndepărtate care, în mod normal, nu au acces la rețeaua fără fir. S-ar putea ca un punct de acces dintr-o locuință sau din sediul unei firme mici să nu acopere toată aria în care utilizatorii au nevoie de conectivitate, de pildă un subsol sau o curte interioară. Plasarea unui repetoar între zonele cu acoperire și cele fără acoperire va asigura conectivitatea pentru întreg spațiul dorit. Repetoarele fără fir umplu golurile de acoperire, permițând roaming-ul pe o suprafață fără goluri.

Un dezavantaj al repetoarelor este, însă, acela că reduc performanța LAN-ului fără fir. Un repetoar trebuie să recepționeze și să retransmită fiecare cadru prin același canal radio, ceea ce dublează efectiv traficul prin rețea. Această problemă se amplifică atunci când sunt utilizate mai multe repetoare, pentru că fiecare dintre acestea va duplica datele transmise. De aceea, asigurați-vă că ați planificat cu măsură folosirea repetoarelor.

Antene

Majoritatea antenelor pentru LAN-urile fără fir sunt omnidirecționale și au câștig scăzut. Aproape toate punctele de acces, routerele și repetoarele sunt echipate standard cu antene omnidirecționale. Antenele omnidirecționale satisfac majoritatea cerințelor de acoperire; totuși, puteți lua în considerare utilizarea opțională a unei antene directive pentru acoperirea unei zone lungi, înguste. În unele cazuri, antena este integrată în placa radio sau în punctul de acces și atunci nu există posibilitatea de a opta. Dacă este necesară utilizarea unei antene directive (câștig ridicat) asigurați-vă că placa radio sau punctul de acces posedă un conector extern pentru antenă.

Sisteme LAN fără fir

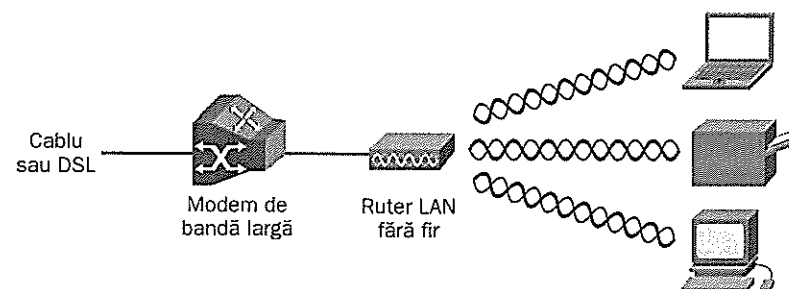
Un sistem LAN fără fir constă dintr-un set de componente și configurări care satisfac necesitățile unei anumite aplicații. Există posibilitatea definirii unui sistem general LAN fără fir pe baza tipurilor mari de aplicații. Să vedem câteva exemple.

LAN-uri fără fir pentru locuințe și sedii de firme mici

Folosirea unei rețele LAN fără fir într-o locuință sau într-un sediu al unei firme mici elimină necesitatea instalării de cabluri pentru a interconecta PC-uri, laptopuri și imprimante. Aproape oricine poate achiziționa componentele potrivite de la un magazin de electronice sau de birotică și poate să instaleze o LAN fără fir. Instalarea și configurarea unei rețele LAN fără fir sunt simple.

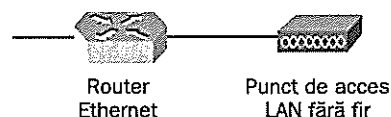
Așa cum se arată în figura 5.4, în general, o LAN fără fir pentru locuințe sau pentru sedii de firme mici include un singur router LAN fără fir care leagă rețeaua la o conexiune Internet de bandă largă, de pildă la DSL sau la un modem de cablu. Raza de acțiune tipică a unei rețele LAN fără fir este potrivită pentru o casă, un apartament sau un sediu mic. Un router este necesar atunci când există mai mult de o singură componentă de rețea. De exemplu, o rețea de locuință constând dintr-un PC, un laptop și o imprimantă, conectate fără fir, necesită utilizarea NAT și DHCP pentru a satisface nevoile de adresare pentru toate dispozitivele.

Figura 5.4. LAN-urile fără fir din locuințe sau din sediile mici au o configurație simplă



De asemenea, într-o locuință sau într-un sediu mic poate funcționa un singur punct de acces, însă acest lucru va permite ca doar un singur dispozitiv să obțină o adresă IP și accesul la Internet. Acest lucru se petrece deoarece majoritatea punctelor de acces nu implementează NAT și DHCP. Combinația dintre un punct de acces și un router legat prin fir va fi, însă, suficientă pentru un router LAN fără fir (vezi figura 5.5). Aceasta poate fi o soluție mai ieftină decât achiziționarea unui router LAN fără fir, dacă aveți deja un punct de acces sau un router conectat prin fir (ori ambele).

Figura 5.5. Combinația dintre un punct de acces LAN fără fir și un router Ethernet oferă aceleași funcționalități ca un router LAN fără fir



Sfat

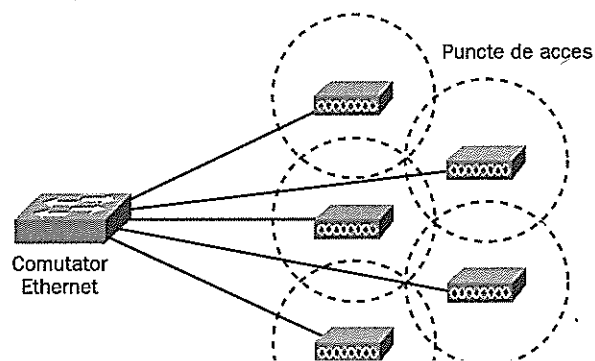


Punctele de acces LAN fără fir și routerele posedă setări de securitate prestabilite, cum ar fi WEP, care sunt dezactivate inițial. Pentru a preveni accesul cuiva, din afara locuinței sau a sediului, la fișierele din rețeaua dumneavoastră, activați elementele de control pentru securitate, atunci când configurați LAN-ul fără fir.

LAN-uri fără fir pentru întreprinderi (pentru sedii de firme mari)

O LAN fără fir pentru o întreprindere este mult mai complicată decât una pentru o locuință sau pentru un sediu mic. Motivul principal este acela că LAN-urile fără fir de companie necesită mai multe puncte de acces, ceea ce presupune existența unui sistem de distribuție dezvoltat care să interconecteze punctele de acces. Așa cum este prezentat în figura 5.6, punctele de acces asigură celulele radio care se suprapun parțial ceea ce permite utilizatorilor să acceseze resursele rețelei cu fir în timp ce se deplasează prin clădire. Această configurație, numită adesea infrastructură mod, este cea mai obișnuită pentru LAN-urile fără fir care acoperă o suprafață mai mare de 2 000 de metri pătrați.

Figura 5.6. LAN-urile fără fir de întreprindere necesită un număr substanțial de cabluri pentru interconectarea punctelor de acces



De exemplu, o LAN fără fir pentru un spital poate să aibă sute de puncte de acces localizate peste tot prin spital. O multitudine de comutatoare Ethernet și de cabluri asociate acestora sunt necesare pentru a le lega împreună. Ca și în cazul altor LAN-uri fără fir de întreprindere, într-un spital probabil că există hardware care oferă servicii DHCP. Prin urmare, o rețea LAN fără fir de întreprindere folosește puncte de acces, nu routere LAN fără fir.

LAN-urile fără fir de întreprindere au nevoie și de mecanisme de securitate sofisticate. În comparație cu necesitățile de securitate pentru locuințe și sedii mici, în cazul acesta se pune accent mai mare pe autentificare și pe criptare. Citiți capitolul 8, intitulat *Securitatea rețelelor fără fir: protejarea resurselor de informații*, pentru a afla mai multe detalii privitoare la securitatea LAN-urilor fără fir.

Sfat



Atunci când instalați o LAN fără fir publică, ori de întreprindere, asigurați-vă că există un specialist care să realizeze o examinare RF a locației pentru a evalua prezența surselor de interferențe RF, pentru a determina pozițiile ideale pentru punctele de acces și pentru a le stabili canalele RF de lucru.

LAN-uri fără fir adecvate pentru pacienți

Centrele de îngrijire a sănătății, cum sunt spitalele și cabinetele medicale, trebuie să păstreze înregistrări exacte pentru a asigura o îngrijire eficientă a pacienților. O greșală banală poate costa viața unui om. Prin urmare, medicii și asistentele medicale trebuie să înregistreze cu grijă rezultatele analizelor, datele fizice, rețetele și operațiile chirurgicale. Înregistrarea pe hârtie a acestor date copleșește adesea personalul medical, ocupându-i 50-70% din timpul de lucru. Utilizarea unui dispozitiv colector de date care transmite fără fir datele către o bază de date centralizată crește semnificativ acuratețea datelor și îmbunătățește capacitatea de accesare a acestora de către persoanele care au nevoie de informații. Acest lucru conduce la o mai bună îngrijire a pacienților.

De asemenea, medicii și asistentele medicale sunt în permanentă mișcare, trecând dintr-o încăpere în alta pentru a se ocupa de pacienți. Utilizarea înregistrărilor electronice pentru pacienți, care oferă posibilitatea de a se introduce, a se vizualiza și a se actualiza date privitoare la aceștia din orice punct al spitalului, îmbunătățește acuratețea și viteza acordării îngrijirilor medicale. Această îmbunătățire a activității medicale se poate realiza punând la



dispoziția fiecărui cadru medical un calculator cu introducere de date prin creion electronic, cum este o tabletă digitalizatoare sau un PDA, cuplat printr-o rețea fără fir la o bază de date care stochează informațiile medicale importante privitoare la pacienți.

Un medic care se ocupă de un pacient din spital, de exemplu, poate trimite o comandă pentru o analiză a sângelui prin introducerea solicitării într-un calculator de mână. Laboratorul primește comanda pe cale electronică și trimite un laborant să preia sângele de la pacient. Laboratorul efectuează analizele solicitate de către medic și introduce rezultatele în fișa medicală electronică a pacientului. Medicul poate verifica ulterior rezultatele prin intermediul calculatorului de mână, de oriunde s-ar afla în spital.

O altă aplicație a rețelelor fără fir în spitale este legată de urmărirea produselor farmaceutice. Utilizarea unui dispozitiv de mână mobil care scanează și tipărește coduri de bare crește în mod spectaculos eficiența și acuratețea operațiunilor legate de produsele farmaceutice, cum ar fi recepționarea, distribuirea, prepararea și inventarierea acestora, precum și urmărirea datelor de expirare. Însă, cel mai important aspect este să se asigure posibilitatea ca personalul medical să poată administra medicamentul adecvat, pacientului care are nevoie de acesta, la momentul oportun. Acest lucru nu este posibil fără utilizarea unei rețele fără fir care să furnizeze servicii pentru baza de date centralizată și pentru dispozitivele mobile pentru colectarea de date.

LAN-uri fără fir publice

O rețea *LAN fără fir publică* permite oricui posedă un dispozitiv de utilizator echipat cu o NIC LAN fără fir să acceseze Internetul. LAN-uri fără fir publice sunt disponibile din majoritatea „punctelor fierbinți”, cum ar fi aeroporturile, centrele de afaceri, hotelurile și porturile de pe glob³. *Punctele fierbinți* de bună calitate sunt acelea pe care oamenii le vizitează cu regularitate ca baze temporare din care doresc să acceseze servicii de rețea.

Notă



Localizați un punct fierbinte apropiat, în care se află o rețea LAN fără fir publică, vizitând <http://www.wi-fihotspotlist.com/>.

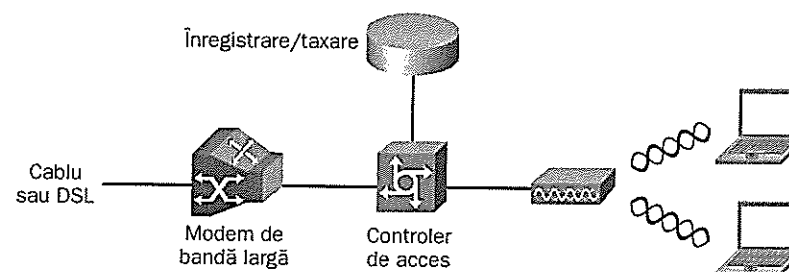
³ Acest lucru este valabil mai curând pentru America de Nord, Europa de Vest și statele avansate din Extremul Orient (n.tr.).

O LAN fără fir publică poate fi folosită de oricine. Acest lucru oferă o sursă de venituri pentru proprietarul punctului fierbinte care poate înregistra abonații (aceștia plătesc o taxă pentru a accesa rețeaua). Totuși, în unele situații, deținătorii punctelor fierbinți pot oferi acces liber la LAN pentru a crește numărul de vizitatori ai locației.

LAN-urile fără fir pentru puncte fierbinți mici sunt simple. De exemplu, proprietarul unei cafenele poate instala un singur router LAN fără fir care realizează interfața cu o conexiune Internet de bandă largă. Această configurație este similară cu aceea utilizată pentru o locuință sau pentru un sediu mic. Accesul liber îi încurajează pe clienți să cumpere cafea și alte bunătăți în timp ce navighează pe Web sau corespundează prin e-mail.

În cazul în care proprietarul punctului fierbinte vrea să taxeze accesul, sistemele LAN fără fir trebuie să includă un controler de acces și funcția de înregistrare și taxare, așa cum se arată în figura 5.7. Atunci când un utilizator își rulează browser-ul Web, controlerul de acces îl redirecționează automat pe acesta la o pagină Web care îi solicită utilizatorului să se conecteze (prin nume de utilizator și parolă) sau să se înscrie ca abonat al serviciului. Opțiunile de înregistrare/taxare pot fi pe minut, pe zi sau pe lună. Sistemul de înregistrare/taxare urmărește utilizarea serviciului și taxează automat cărțile de credit.

Figura 5.7. LAN-urile fără fir publice necesită componente care depășesc scopul tehnicilor pentru rețele fără fir



Punctele fierbinți de mari dimensiuni necesită mai multe puncte de acces, comparabil cu o rețea LAN fără fir de întreprindere. LAN-urile fără fir publice, care cuprind câteva locații, necesită, de asemenea, sisteme sofisticate de control al accesului și de înregistrare/taxare. Un mare lanț hotelier, de exemplu, poate instala LAN-uri fără fir publice în sute de locații diferite. Utilizatorii pot obține abonamente lunare pentru acces și vor putea utiliza serviciile din oricare dintre hoteluri. În această situație, funcția de control al accesului necesită existența unui server centralizat care stochează informațiile pentru autentificare, autorizare și evidență (în limba engleză: authentication, authorization and accounting — acronim AAA).

LAN-urile fără fir în hoteluri

Pentru a oferi acoperire fără fir clienților lor, hotelurile instalează puncte de acces în sălile de conferințe, sălile de bal, sălile pentru întâlniri de afaceri, holuri, zonele din preajma piscinelor și în camerele de oaspeți.

O rețea LAN fără fir de hotel poate oferi oaspeților, pe perioada șederii lor, următoarele servicii:

- Navigarea pe Web în timp ce se află la piscină sau într-un centru de fitness.
- Acces protejat, de la distanță, din camera de hotel, la rețelele de corporație ale acestora.
- Revizuirea online a programărilor și obținerea de informații de orientare prin localitate/zonă.
- Partajarea unei conexiuni Internet de mare viteză cu mai mulți participanți la o conferință.
- Tipărirea de la distanță, din camerele de oaspeți, la imprimante aflate în centrul de afaceri.
- Realizarea de video conferințe cu asociați sau membri ai familiei.

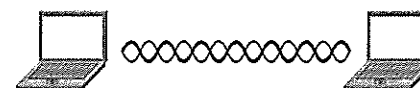
Conducerea și administrația hotelurilor poate, de asemenea, să beneficieze de avantaje importante datorate LAN-urilor fără fir. De exemplu, instalarea unei rețele LAN fără fir face ca realizarea următoarelor sarcini să fie mai ușoară și mai eficientă:

- Inspectarea camerelor pentru a verifica dacă totul este în ordine și dacă nu s-au produs distrugereri în acestea. Conducerea poate verifica camera și poate trimite informația printr-o buclă inversă, către un calculator central, printr-un PDA cu interfață 802.11.
- Realizarea de inspecții de securitate și de siguranță pentru a se asigura că: ușile sunt închise, extintoarele sunt încărcate, luminile pentru cazuri de urgență funcționează corespunzător și așa mai departe. Toate informațiile pot fi actualizate în timp real, economisind timp și evitând posibilitatea de apariție a erorilor.
- Menținerea contactului cu lucrătorii de întreținere prin utilizarea de telefoane LAN fără fir. Administrația poate contacta echipele de întreținere oricând este nevoie, rezultând timpi mai scurți de răspuns la solicitări.

LAN-uri fără fir ad-hoc

O LAN fără fir ad-hoc, așa cum este ilustrat în figura 5.8, nu utilizează puncte de acces. În schimb, fiecare dispozitiv individual de utilizator comunică direct cu un altul. Avantajul acestei configurații este acela că utilizatorii pot forma în mod spontan, cu rapiditate, o LAN fără fir. Rețelele ad-hoc sunt cunoscute frecvent și sub numele de rețele de la egal la egal.

Figura 5.8. LAN-urile fără fir ad-hoc oferă o configurare și o funcționare simple



De exemplu, o LAN fără fir ad-hoc ușurează sarcina cuiva de a transfera un fișier de mari dimensiuni unui asociat aflat în aceeași sală de conferințe, în care nu este disponibilă o infrastructură LAN fără fir. Fiecare utilizator trebuie doar să-și configureze NIC-ul radio pentru funcționare în *modul ad-hoc* și conexiunile se realizează în mod automat. În unele cazuri, utilizatorii trebuie să se asigure de faptul că adresele lor IP sunt stabilite în aceeași subrețea.

Modul ad-hoc este avantajos și pentru asigurarea serviciilor de urgență, atunci când funcționarea are loc în zone unde realizarea unui sistem de distribuție pentru interconectarea punctelor de acces nu este practică. Un grup de asistență în caz de dezastre, de exemplu, poate configura cu rapiditate conexiuni de rețea între membri echipei care lucrează în zone afectate de uragane, inundații sau atacuri teroriste.

Tehnici LAN fără fir

802.11 și HiperLAN/2 sunt cele mai comune standarde pentru LAN-urile fără fir. Să examinăm fiecare dintre aceste standarde.

802.11

Standardul IEEE 802.11 specifică un *control al accesului la mediu* (în limba engleză: *medium access control* — acronim *MAC*) comun și câteva straturi fizice pentru LAN-urile fără fir. Standardul 802.11 inițial a devenit disponibil în 1997, însă LAN-urile fără fir nu au început să se răspândească până când prețurile nu au scăzut spectaculos, în anul 2001. Grupul de lucru IEEE 802.11 își continuă activitatea pentru a dezvolta standardul în scopul îmbunătățirii performanțelor și securității pentru LAN-urile fără fir.



Notă

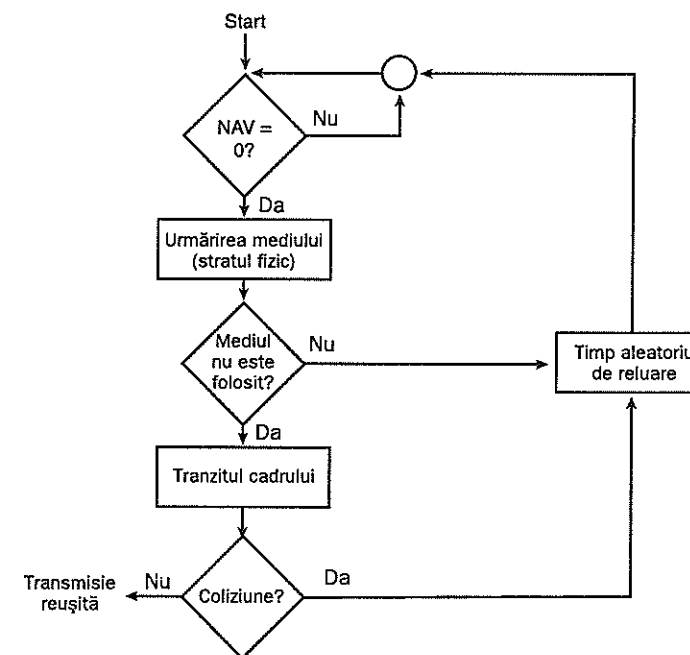
Standardul 802.11 specifică și folosirea unui strat fizic bazat pe lumină infraroșie; însă, nu există astăzi pe piață produse care să se conformeze acestei versiuni a standardului.

Stratul MAC 802.11

Standardul 802.11 specifică un singur strat MAC care furnizează o varietate de funcții pentru a asigura operarea LAN-urilor fără fir bazate pe 802.11. Stratul MAC administrează și întreține comunicațiile dintre stațiile 802.11 (plăcile radio de rețea și punctele de acces) prin coordonarea accesului la un mediu aerian partajat. Adesea considerat ca fiind creierul rețelei, stratul MAC 802.11 controlează un anumit strat fizic 802.11, cum ar fi 802.11a, 802.11b sau 802.11g pentru a realiza sarcinile legate de urmărirea (perceperea) mediului și de transmisia și recepția cadrelor 802.11.

Înainte de a transmite cadrele, o stație trebuie, mai întâi, să obțină accesul la mediu, care este canalul radio pe care îl partajează stațiile. Standardul 802.11 definește două forme de acces la mediu: *funcția de coordonare distribuită* (în limba engleză: *distributed coordination function* — acronim *DCF*) și funcția de coordonare a punctului (în limba engleză: *point coordination function* — acronim *PCF*). DCF este obligatoriu și este bazat pe protocolul *CSMA/CA* (*carrier sense multiple access with collision avoidance* — *acces multiplu cu urmărirea purtătoarei și evitarea coliziunilor*). În cazul utilizării DCF, stațiile 802.11 își dispută accesul la mediu și încearcă să transmită cadre atunci când nu transmite nici o altă stație (vezi figura 5.9). Dacă o stație transmite un cadru, celelalte stații așteaptă până când se eliberează canalul.

Figura 5.9. DCF oferă o formă distribuită de acces la mediu



Ca o condiție pentru accesarea mediului (vezi figura 5.9), stratul MAC verifică valoarea pe care o are vectorul de alocare a rețelei (în limba engleză: *network allocation vector* — acronim *NAV*). Acesta este un contor aflat în fiecare stație a cărui valoare reprezintă intervalul de timp care a fost necesar pentru transmiterea cadrului anterior. Valoarea NAV trebuie să fie 0 înainte ca o stație să poată încerca să transmită un cadru. Înainte de a trimite cadrul, stația calculează intervalul de timp necesar transmiterii acestuia pe baza dimensiunii cadrului și pe baza vitezei de transmisie a datelor. Stația plasează valoarea care reprezintă acest interval de timp în câmpul durată din antetul cadrului. Atunci când alte stații recepționează cadrul, acestea examinează valoarea din câmpul durată și o folosesc ca bază pentru stabilirea valorilor NAV corespunzătoare. Acest proces rezervă mediul pentru stația transmițătoare.

Un aspect important al DFC este ceasul pentru reluarea aleatoare pe care stația îl folosește dacă sesizează că mediul nu este liber. Dacă canalul este utilizat, stația trebuie să aștepte o perioadă de timp aleatoare înainte de a încerca din nou să acceseze mediul. Acest lucru asigură faptul că stațiile care așteaptă să trimită date nu vor începe transmisiile în același moment. Întârzierea aleatoare face ca stațiile să



aștepte perioade diferite de timp și evită ca acestea să verifice mediul exact în același moment de timp și, găsind canalul liber, să transmită simultan ceea ce ar conduce la producerea de coliziuni. Ceasul de reluare reduce semnificativ numărul de coliziuni și de retransmisii corespunzătoare, mai ales atunci când crește numărul de utilizatori activi.

În cazul LAN-urilor bazate pe unde radio, o stație emițătoare nu poate asculta pentru a detecta coliziunile în timp ce transmite date, întrucât deoarece stația nu poate avea receptorul activ în timp ce transmite un cadru. Prin urmare, stația receptoare trebuie să transmită o confirmare (în limba engleză: acknowledgement — acronim ACK) dacă sesizează că în cadrul recepționat nu există erori. Dacă stația emițătoare nu recepționează un semnal ACK într-o perioadă de timp bine stabilită, aceasta va presupune că s-a produs o coliziune (sau o interferență RF) și va retransmite cadrul respectiv.

Pentru a putea asigura o livrare în timp restrâns a cadrelor de date cum ar fi cele pentru transmisiile video, standardul 802.11 definește forma opțională de control al accesului PCF, în care punctul de acces acordă accesul la mediu unei anumite stații prin selectarea stației în timpul perioadei de timp în care stațiile nu se concurează pentru a emite. Stațiile nu pot transmite cadre dacă nu au fost mai întâi selectate de punctul de acces. Perioada de timp în care se realizează traficul de date pe baza PCF (dacă acesta este permis) apare alternativ între perioadele de concurență pentru transmisie.

Punctul de acces selectează stațiile pe baza unei liste de selecție, apoi comută la o perioadă de concurență pe parcursul căreia stațiile folosesc DCF. Acest proces permite realizarea funcționării atât în modul sincron cât și în cel asincron. NIC-urile fără fir și punctele de acces aflate astăzi pe piață nu implementează, însă, PCF.

O problemă legată de PCF este aceea că există puțini producători care îl integrează în produsele lor. Prin urmare, în general, acesta nu constituie o opțiune disponibilă pentru utilizatori. Este însă posibil ca produsele viitoare să integreze PCF cu scopul de a oferi mecanisme legate de calitatea serviciilor (QoS).

Secțiunile următoare rezumă principalele funcții MAC 802.11.

Scanarea

Standardul 802.11 definește atât scanarea activă, cât și pe cea pasivă, pentru situația în care o placă NIC radio caută punctele de acces. Scanarea pasivă este obligatorie atunci când fiecare placă NIC scanează canale diferite pentru a găsi cel

mai bun semnal de punct de acces. Punctele de acces difuzează periodic un semnal far, iar NIC-ul radio recepționează acest semnal atunci când scanează, și evaluează puterea acestuia. Aceste semnale conțin informații privitoare la punctul de acces care includ SSID și viteza de transmisie asigurată de acesta. NIC-ul radio poate folosi aceste informații, alături de puterea semnalului, pentru a face comparație între punctele de acces și pentru a decide pe care dintre acestea îl va utiliza.

Scanarea activă, care este opțională, este similară cu cea pasivă, cu excepția faptului că NIC-ul radio este cel care inițiază procesul prin difuzarea unui cadru de sondare, iar punctele de acces din raza de acțiune a acestuia emit un răspuns de sondare. Scanarea activă permite unei NIC radio să primească imediat răspunsul de la punctele de acces, fără să mai aștepte transmisia unui semnal far. Însă, problema constă în faptul că scanarea activă impune o încărcare suplimentară a rețelei datorită transmisiilor de sondare și datorită transmisiilor cadrelor corespunzătoare de răspuns.

Stațiile care lucrează în modul ad-hoc sunt numite, de către standardul 802.11, set independent de servicii de bază. În acest mod de operare, una dintre stații transmite un semnal far, care informează noile stații asupra prezenței rețelei. Responsabilitatea transmiterii semnalului far se bazează pe faptul că fiecare stație așteaptă să treacă intervalul de timp dintre două semnale far și o perioadă suplimentară aleatorie de timp. O stație transmite un semnal far, dacă, după trecerea intervalului de timp dintre două semnale far plus perioada aleatorie, nu recepționează un semnal far emis de altă stație. Acest proces distribuie responsabilitatea transmiterii de semnale far între toate stațiile.

Autentificarea

Autentificarea este un proces de dovedire a identității, iar standardul 802.11 specifică două forme: autentificarea sistemelor deschise și autentificarea cu cheie partajată. Autentificarea pentru sisteme deschise este obligatorie și este un proces în doi pași. NIC-ul radio inițiază procesul prin transmiterea unui cadru solicitare de autentificare către punctul de acces. Punctul de acces răspunde printr-un cadru răspuns de autentificare care conține aprobarea sau respingerea autentificării indicată prin starea câmpului cod din corpul cadrului.

Autentificarea cu cheie partajată este un proces opțional, în patru pași, prin care autentificarea este bazată pe verificarea faptului că dispozitivele care solicită autentificarea posedă cheia WEP corectă. NIC-ul radio inițiază procesul prin transmiterea unui cadru solicitare de autentificare către punctul de acces. Punctul de acces plasează apoi un text pentru recunoaștere în corpul cadrului de răspuns și îl

transmite NIC-ului radio. Placa de rețea radio folosește propria cheie WEP pentru a cripta textul de recunoaștere și apoi îl trimite înapoi la punctul de acces printr-un alt cadru de autentificare. Punctul de acces decriptează textul de recunoaștere și îl compară cu textul inițial. Dacă textele sunt identice, punctul de acces presupune că NIC-ul radio posedă cheia corectă. Punctul de acces finalizează procesul prin transmiterea unui cadru de autentificare către placa de rețea radio, cadru care conține aprobarea sau respingerea accesului. Însă, mulți hackeri știu cum să treacă de autentificarea cu cheie partajată, așa că nu este o idee bună să depindeți de aceasta pentru un nivel înalt de securitate.

Asocierea

O dată autentificată, placa de rețea radio trebuie să se asocieze cu punctul de acces înainte de a transmite cadrele de date. **Asocierea** este necesară pentru realizarea unei sincronizări între placa radio și punctul de acces, privitoare la informații importante, cum ar fi vitezele de transmisie de date asigurate. NIC-urile radio inițiază asocierea prin transmiterea unui cadru solicitare de asociere, care conține elemente cum ar fi SSID și vitezele de transmisie care pot fi realizate. Punctul de acces răspunde prin transmiterea unui cadru răspuns de asociere care conține un identificador de asociere împreună cu alte informații privitoare la punctul de acces. O dată ce placa radio și punctul de acces au încheiat procesul de asociere, vor putea să transmită cadre de la unul la celălalt.

WEP⁴

În cazul activării opționale a criptării WEP, NIC-ul fără fir criptează corpul (nu și antetul) fiecărui cadru, înainte de a-l transmite, utilizând o cheie comună; iar stația receptoare decriptează cadrul după ce îl primește folosind cheia comună. Standardul 802.11 nu specifică o metodă de distribuire a cheii, ceea ce face ca LAN-urile fără fir 802.11 să fie vulnerabile la cei care „trag cu urechea”. Versiunea 802.11i a standardului, îmbunătățește, însă, securitatea rețelelor 802.11 prin încorporarea în standard a versiunilor 802.1x și a unei criptări mai solide.

RTS/CTS⁵

Funcția opțională solicitare-pentru-transmisie (request-to-send) și liber-pentru-transmisie (clear-to-send) permite punctului de acces să controleze folosirea mediuului pentru stațiile care au activată funcția RTS/CTS. În cazul majorității NIC-urilor radio, utilizatorii pot stabili un prag pentru dimensiunea maximă a cadrului de la care NIC-urile radio activează funcția RTS/CTS. De exemplu, o dimensiune a pragului

⁴ În limba engleză, *wired equivalent privacy* (n.tr.).

cadrului de 1000 de octeți activează funcția RTS/CTS pentru cadre mai mari de 1000 de octeți. Utilizarea funcției RTS/CTS micșorează problemele ascunse, legate de nod (atunci când două sau mai multe NIC-uri radio nu se pot auzi reciproc, fiind asociate la același punct de acces).

Dacă placa de rețea radio activează funcția RTS/CTS, trimite mai întâi un cadru RTS către punctul de acces, înainte de a transmite un cadru de date. Punctul de acces răspunde, apoi, cu un cadru CTS care indică plăcii radio faptul că poate transmite cadrul de date. Punctul de acces include în câmpul durată al antetului cadrului CTS o valoare care le oprește pe celelalte stații să transmită până când placa radio care a inițiat funcția RTS își poate transmite cadrul de date. Acest lucru conduce la evitarea coliziunilor dintre nodurile ascunse. Stabilirea unei înțelegeri prin intermediul funcției RTS/CTS continuă pentru fiecare cadru, atâta vreme cât dimensiunea cadrului depășește pargul stabilit pentru respectiva placă radio.

Modul economie de energie⁶

Modul opțional economie de energie poate fi activat de utilizator pentru a permite plăcii radio să-și conserve bateriile atunci când nu trebuie să transmită date. Atunci când acest mod este activ, placa radio va anunța punctul de acces de intenția sa de a intra în starea de „somm” prin intermediul unui bit de stare localizat în antetul fiecărui cadru. Punctul de acces ia notă de fiecare NIC radio care așteaptă să intre în modul economie de energie și stochează în buffere pachetele care corespund stației „adormite”.

Pentru a primii totuși cadrele cu date, placa „adormită” trebuie să se „trezească” periodic (la momentul potrivit) pentru a recepționa transmisiile regulate de semnale far care vin dinspre punctul de acces. Aceste semnale far indică dacă stațiile „adormite” au cadre stocate în bufferele punctului de acces, cadre care așteaptă să fie livrate la destinațiile lor. NIC-urile radio care au cadre în așteptare le vor solicita de la punctul de acces. După ce recepționează cadrele, placa radio se poate întoarce la starea de „somm”.

Fragmentarea

Funcția opțională de fragmentare permite unei stații 802.11 să divizeze pachetele de date în cadre mai mici. Acesta pentru a evita nevoia de a retransmite cadre de mari dimensiuni în prezența interferenței RF. Este probabil ca erorile de biți rezultate din interferența RF să afecteze un singur cadru, și atunci se va produce o supraîncărcare mai scăzută a rețelei dacă este retransmis un cadru mai mic în locul unui mare. Ca și în cazul utilizării RTS/CTS, utilizatorii pot stabili un prag al dimensiunii maxime a cadrului pentru momentul în care placa radio activează funcția de fragmentare.

⁶ În limba engleză, *Power Save Mod* (n.tr.).

Dacă dimensiunea cadrului este mai mare decât pragul, placa radio va sparge pachetul în mai multe cadre, fiecare dintre acestea având o dimensiune sub valoarea de prag.

Straturile fizice 802.11

Câteva straturi fizice 802.11 satisfac o varietate de cerințe ale aplicațiilor. Secțiunile următoare oferă un rezumat privitor la fiecare strat fizic 802.11.

Standardul inițial 802.11

Standardul inițial 802.11, ratificat în 1997, include straturile fizice *salturi de frecvență în spectru larg* (în limba engleză: *frequency hopping spread spectrum* – acronim FHSS) și *secvență directă în spectru larg* (în limba engleză: *direct sequence spread spectrum* — acronim DSSS), care operează în banda de 2,4 GHz, cu viteze de transmisie de până la 2Mbps. FHSS transmite un semnal de bandă largă care se întinde pe toată banda de 2,4 GHz. Există posibilitatea de a regla punctele de acces FHSS la nu mai puțin de 15 moduri diferite de salturi de frecvență care nu interferă unele cu altele, ceea ce permite ca un număr de până la 15 puncte de acces să poată opera efectiv în aceeași zonă.

Deoarece versiunea curentă FHSS 802.11 are o viteză maximă de transmisie a datelor de numai 2 Mbps, nu există multe companii care comercializează soluții FHSS pentru LAN-uri fără fir de interior (în limba engleză: indoor). Acum sunt disponibile LAN-uri fără fir mai rapide: 802.11a, 802.11b și 802.11g. De asemenea, FHSS nu interoperează cu nici unul dintre celelalte straturi fizice 802.11. Însă, FHSS oferă tocmai soluția necesară pentru sistemele punct-la-multe-puncte, exterioare (în limba engleză: outdoor). Aceasta deoarece FHSS este mai puțin sensibil la interferențele RF care pot fi prezente în mediile exterioare clădirilor.

Rețelele DSSS 802.11 funcționează tot numai până la 2 Mbps, dar interoperează cu stratul fizic 802.11b, care este mai nou. Prin urmare, un utilizator care are o placă radio DSSS 802.11 în laptopul său se poate conecta la un punct de acces 802.11b. Însă, această situație este improbabilă deoarece NIC-urile radio DSSS 802.11 nu mai sunt comercializate în prezent.

802.11a

Către sfârșitul anului 1999, IEEE a lansat 802.11a, care definește funcționarea în banda de 5 GHz folosind multiplexarea prin divizarea ortogonală a frecvenței (OFDM) cu viteze de transmisie de până la 54 Mbps. Însă, produsele nu au devenit disponibile până în 2000, în primul rând din cauza dificultăților legate de dezvoltarea

802.11a funcționează la viteze de transmisie de până la 54 Mbps, în banda de 5 GHz, folosind OFDM și având o rază de acțiune de până la 30 de metri (în funcție de viteza efectivă de transmisie a datelor). Punctele de acces 802.11a și NIC-urile radio 802.11a au devenit disponibile doar către sfârșitul lui 2001; de aceea, LAN-urile fără fir, bazate pe 802.11a, instalate până în ziua de azi, sunt relativ puține prin comparație cu cele bazate pe 802.11b. Din această cauză, trebuie să luați în considerație, cu atenție, aspectele legate de interoperare, care ar putea rezulta dacă alegeți să instalați o rețea 802.11a.

Un avantaj important al standardului 802.11a este acela că oferă cea mai mare capacitate datorată celor 12 canale separate, care nu se suprapun. Acest lucru face ca rețelele 802.11a să fie o bună alegere pentru asigurarea unei concentrări mari de utilizatori și pentru realizarea unor aplicații de înaltă performanță, cum ar fi transmisia informației video în flux continuu. În afară de faptul că sunt mai performante decât sistemele 802.11b, sistemele 802.11a au capacități mai mari decât cele bazate pe 802.11g.

Un alt avantaj al standardului 802.11a este acela că banda de 5GHz nu este aglomerată, ceea ce permite utilizatorilor să atingă nivele înalte de performanță. Majoritatea dispozitivelor care produc interferențe, cum sunt cuptoarele cu microunde și telefoanele fără fir, operează în banda de 2,4 GHz. Având un potențial de interferență RF mai scăzut, instalarea de astfel de LAN-uri fără fir este mai puțin riscantă.

O problemă potențială a rețelelor 802.11a este legată de raza de acțiune limitată, în principal datorită funcționării într-o bandă de frecvență mai înaltă, cea de 5 GHz. La 54 Mbps, veți avea o rază de acțiune mai mică de 30 de metri în majoritatea clădirilor. Acest lucru necesită un număr mai mare de puncte de acces pentru acoperirea completă a clădirii, decât în cazul utilizării unui sistem 802.11b.

Însă, dacă comparați funcționarea unui sistem 802.11b cu cea a unui sistem 802.11a, un utilizator 802.11a va avea o viteză de transmisie a datelor mai mare aflându-se la aceeași distanță față de punctul de acces ca și utilizatorul 802.11b, până când utilizatorul 802.11a depășește distanța la care pierde conectivitatea. Însă, utilizatorul 802.11b va putea să continue să funcționeze la viteze de transmisie mai scăzute — cum ar fi 1 sau 2 Mbps — la distanțe mai mari de punctul de acces decât utilizatorul 802.11a.



O problemă clară este aceea că standardele 802.11a și 802.11b/g nu sunt compatibile. De exemplu, un utilizator echipat cu o placă radio 802.11b nu se poate asocia cu un punct de acces 802.11a, și scenariul opus este adevărat. Producătorii rezolvă această problemă prin introducerea plăcilor radio multimod, care implementează atât 802.11a cât și 802.11b.

Un modulator 802.11a convertește semnalul binar într-o formă de undă analogică prin intermediul unor tipuri diferite de modulare, care depind de alegerea făcută pentru viteza de transmisie a datelor. De exemplu, pentru funcționarea la 6 Mbps, modulatorul utilizează modularea binară de fază (în limba engleză: binary phase shift keying — acronim BPSK), care decalează faza semnalului emițătorului pentru a reprezenta diferite tipare de biți de date. La viteze de transmisie a datelor mai mari, cum ar fi 54 Mbps, este folosită modularea în fază și amplitudine (QAM) pentru a reprezenta biții de date prin varierea semnalului emițătorului la diverse niveluri de amplitudine, suprapusă peste decalarea fazei.

802.11b

O dată cu standardul 802.11a, IEEE a ratificat și standardul 802.11b, care este o extensie de viteză de transmisie mai înaltă a standardului inițial, cu secvență directă în banda de 2,4 GHz, și care funcționează la viteze de transmisie de până la 11 Mbps. Punctele de acces 802.11b și NIC-urile radio 802.11b au devenit disponibile din 1999; de aceea, majoritatea LAN-urilor fără fir instalate la acest moment se conformează standardului 802.11b.

Un avantaj semnificativ al rețelelor 802.11b este acela al razei relativ lungi de acțiune. Utilizând standardul 802.11b puteți obține o rază de acțiune de 100 de metri în majoritatea instalărilor interioare. Raza de acțiune superioară permite desfășurarea de LAN-uri fără fir care folosesc mai puține puncte de acces, prin comparație cu o rețea 802.11a, pentru a acoperi o locație.

Un dezavantaj al rețelelor 802.11b este acela că sunteți limitat la numai trei canale, care nu se suprapun, în banda de 2,4 GHz. Standardul 802.11 specifică 14 canale de transmisie (în SUA sunt disponibile numai canalele de la 1 la 11) pentru configurarea punctelor de acces; însă, fiecare canal ocupă cam o treime din întreaga bandă de 2,4 GHz, atunci când este transmis un semnal. Majoritatea companiilor utilizează numai canalele 1, 6 și 11 pentru a se asigura că punctele de acces nu interferă unele cu altele. Acest lucru limitează capacitatea globală a rețelelor 802.11b, ceea ce le face să fie cele mai potrivite pentru realizarea de aplicații de performanțe medii, cum ar fi e-mail și navigarea pe Web.

Un alt dezavantaj al sistemelor 802.11b este cel legat de potențialul de interferență RF datorat altor dispozitive radio. De exemplu, un telefon fără fir care funcționează la 2,4 GHz produce interferențe puternice cu o LAN fără fir 802.11b, ceea ce reduce semnificativ performanțele. Cuptoarele cu microunde și alte dispozitive care funcționează în banda de 2,4 GHz pot, de asemenea, să producă interferențe.

Rețelele 802.11b folosesc DSSS pentru a dispersa semnalul care transmite un cadru de date pe o porțiune de 22 MHz din banda de frecvențe de 2,4 GHz. Acest lucru conduce la o mai mare imunitate la interferența RF, prin comparație cu semnalele de bandă îngustă, acesta fiind motivul pentru care FCC consideră că funcționarea sistemelor în spectru larg se poate realiza fără licență.

Modulatorul 802.11b convertește semnalul binar într-o formă de undă analogică prin intermediul unor tipuri diferite de modulare, care depind de alegerea făcută pentru viteza de transmisie a datelor. De exemplu, în cazul funcționării la 1 Mbps, modulatorul folosește modularea de fază diferențială binară (în limba engleză: differential binary phase shift keying — acronim DBPSK). Acest tip de modulare nu este atât de complicat pe cât este numele său. Modulatorul, pur și simplu, decalează faza semnalului emițătorului pentru a face distincție între cifrele binare 1 și cifrele binare 0 din fluxul de date.

Pentru transmisiile de 2 Mbps, modulatorul utilizează modularea de fază diferențială în cvadratură (în limba engleză: differential quadrature phase shift keying — acronim DQPSK) care este similară cu DBPSK cu excepția faptului că sunt utilizate patru defazaje pentru a reprezenta fiecare pereche posibilă de biți de date (00, 01, 10 și 11). Acest proces „deștept” permite ca fluxul de date să fie transmis la 2 Mbps utilizând aceeași valoare a lărgimii de bandă folosită la transmisiile de 1 Mbps. Modulatorul folosește metode similare pentru a emite la vitezele de transmisie ale datelor mai ridicate, cum sunt cele de 5,5 Mbps și 11 Mbps.

802.11g

IEEE a ratificat standardul 802.11g în 2003, acesta fiind compatibil cu 802.11b și crescând performanțele până la 54 Mbps, în banda de 2,4 GHz, folosind OFDM.

Un avantaj important al standardului 802.11g este acela că este compatibil cu mai vechiul standard 802.11b. Companiile care posedă rețele 802.11b pot, în general, să modernizeze punctele de acces pentru a deveni conforme cu standardul 802.11g, prin intermediul unor modernizări simple de software și hardware. Acest lucru oferă o cale eficientă de migrare a LAN-urilor fără fir. Există, însă, o problemă legată de faptul că prezența dispozitivelor client 802.11b, într-o rețea 802.11g, necesită mecanisme de protecție care limitează performanțele întregii LAN fără fir. Problema



apare pentru că dispozitivele 802.11b nu pot înțelege transmisiile dispozitivelor 802.11g datorită diferențelor dintre tipurile de modulare. Prin urmare, ambele tipuri de dispozitive trebuie să anunțe iminenta utilizare a mediului folosind unui tip de modulare care este, de obicei, înțeles.

¹ Dezavantajele rețelelor 802.11b, cum ar fi potențialul de interferențe RF și limitarea la trei canale care nu se suprapun, există, în continuare, și la rețelele 802.11g datorită funcționării în banda de 2,4 GHz. Prin urmare, rețelele 802.11g au o capacitate restrânsă, prin comparație cu rețelele 802.11a.

2,4 GHz sau 5 GHz?

Atunci când instalează o LAN fără fir, companiile trebuie să decidă dacă vor utiliza NIC-uri și puncte de acces proiectate să funcționeze în banda de 2,4 GHz, în cea de 5 GHz — sau în ambele. Nu cu multă vreme în urmă, alegerea benzii de frecvență era simplă, pentru că erau disponibile numai produse care funcționau la 2,4 GHz (802.11b). Acum, sunt disponibile componente 802.11b și componente 802.11g care operează, și unele și altele, în banda de 2,4 GHz, precum și componente 802.11a care folosesc banda de 5 MHz. Această situație poate produce confuzie la proiectarea unei LAN fără fir, așa că aruncați o privire asupra a ceea ce este necesar să aveți în vedere atunci când luați această decizie critică.

Atunci când evaluați argumentele pro și contra sistemelor care funcționează la 2,4 GHz sau la 5 GHz, pentru început, asigurați-vă că ați definit cerințele. Acest lucru oferă o bază solidă pentru definirea tuturor elementelor de proiectare. În absența unor cerințe exacte, veți lua o decizie nefondată.

În continuare sunt enumerate cerințele care trebuie luate în considerație atunci când alegeți între soluțiile care operează la 2,4 GHz și cele care operează la 5 MHz:

- **Poziția geografică** — Trebuie avută în vedere poziția geografică a locației în care va funcționa LAN-ul fără fir. LAN-urile fără fir la 2,4 GHz sunt aprobate prin reglementări în majoritatea statelor lumii; însă, utilizarea LAN-urilor fără fir la 5 GHz este întrucâtva limitată. De exemplu, SUA acceptă funcționarea LAN-urilor fără fir la 5 GHz, însă alte state nu o permit. Locația dumneavoastră ar putea să vă impună să utilizați banda de 2,4 GHz, fără a ține seama de alte cerințe.
- **Performanța** — Banda de 5 MHz are mult mai mult spectru la dispoziție. Fiecare dintre cele 12 canale ale acestei benzi, care nu se suprapun, au o lărgime de bandă de 20 MHz. Aceasta înseamnă că performanțele sunt semnificativ mai bune prin comparație cu banda de 2,4 GHz. Întreaga lărgime a benzii de 2,4 GHz este de numai 80 MHz, ceea ce permite existența a numai trei canale care să nu se suprapună. Dacă performanța înaltă este o cerință importantă, veți înclina către banda de 5 GHz.
- **Dimensiunile clădirii** — În general, pe măsură ce frecvența de transmisie crește, raza de acțiune descrește. Prin urmare, sistemele care funcționează la 5 GHz au, în principiu, o rază de acțiune mai mică decât cele care funcționează în banda de 2,4 GHz. Alegerea

unei LAN fără fir la 5 GHz poate necesita un număr mai mare de puncte de acces, ceea ce poate conduce la costuri mai mari. Prin urmare, ați putea obține beneficii prin instalarea în clădirile mai mari a sistemelor care funcționează la 2,4 GHz, în cazul în care o performanță ridicată nu este decisivă. Rețineți, totuși, că sistemele care funcționează la 5 GHz pot avea raze de acțiune egale, sau chiar mai mari, în anumite situații.

- **Interferența RF** — În cazul LAN-urilor fără fir care funcționează la 2,4 GHz se pot produce interferențe datorită telefoanelor fără fir, cuptoarelor cu microunde sau altor LAN-uri fără fir. Semnalele care interferează produc o scădere a performanței LAN-ului fără fir 802.11b, datorită blocării periodice a accesului la mediul partajat pentru utilizatori și pentru punctele de acces. Dacă nu este posibil ca potențialul de interferență să fie redus la un nivel acceptabil, trebuie să aveți în vedere instalarea unui sistem la 5 MHz, care este relativ liber de surse de interferență. Există acum pe piață unele telefoane care operează în banda de 5 MHz, dar aceste interferențe sunt mult mai ușor de evitat deoarece standardul 802.11a oferă multe canale de transmisie care nu se suprapun.
- **Interoperabilitatea** — Sistemele la 2,4 GHz și cele la 5 GHz nu sunt compatibile în mod direct și există puțini utilizatori și puține puncte de acces care funcționează în banda de 5 MHz. În consecință, instalarea unei rețele la 2,4 GHz poate fi cea mai bună soluție, dacă nu dețineți controlul asupra tipurilor de NIC-uri pe care utilizatorii le pot avea în PDA-urile și laptopurile lor. Acest lucru se aplică de cele mai multe ori în cazul LAN-urilor fără fir din universități și din punctele fierbinți publice. Aplicația dumneavoastră vă poate cere să implementați versiunea de 2,4 GHz pentru a asigura accesul utilizatorilor echipați în conformitate cu standardul 802.11b, care sunt mult mai des întâlniți.

Producătorii oferă și NIC-uri radio și puncte de acces care funcționează în bandă dublă, ceea ce reduce problemele legate de interoperabilitate. Un utilizator echipat cu o NIC radio în bandă dublă se poate asocia atât cu un punct de acces la 2,4 GHz (802.11b/g) cât și cu unul la 5 GHz (802.11a). Pe măsură ce un număr tot mai mare de utilizatori își echipează dispozitivele cu NIC-uri radio în bandă dublă, problemele legate de interoperabilitate se vor diminua.

- **Securitate** — Securitatea LAN-urilor fără fir constituie o mare preocupare pentru majoritatea companiilor. Prin minimizarea propagării undelor radio în afara zonei controlate dintr-o clădire (sau dintr-un grup de clădiri), rețeaua fără fir va deveni mai sigură deoarece se reduce posibilitatea accesării acesteia de către cei care vor „să tragă cu urechea” sau de către cei care pun la cale atacuri de tip negare de serviciu (în limba engleză: denial of service — acronim DoS). Prin urmare, sistemele care funcționează la 5 GHz pot asigura o protecție sporită prin comparație cu cele la 2,4 GHz, datorită razei lor de acțiune mai restrânsă.

În majoritatea cazurilor, probabil că veți ajunge la concluzia că sistemele la 2,4 GHz sunt calea de urmat pentru aplicațiile uzuale de firmă. Produsele care funcționează la 2,4 GHz sunt fără îndoială ieftine și sunt capabile să satisfacă majoritatea cerințelor aplicației. Totuși, utilizarea unui sistem care operează la 5 GHz este mai avantajoasă în unele situații, cum ar fi în zonele dens populate cu utilizatori sau în cazul aplicațiilor multimedia.



Wi-Fi

Wi-Fi Alliance, care și-a început activitatea sub numele de Wireless Ethernet Compatibility Alliance (WECA), este o organizație internațională nonprofit care se concentrează asupra marketingului și interoperabilității produselor pentru LAN-uri fără fir 802.11. Wi-Fi Alliance este grupul care a impus termenul Wi-Fi pentru a desemna toate formele de rețele bazate pe 802.11, cum ar fi rețelele 802.11a, 802.11b, 802.11g sau oricare altele care vor deveni disponibile în viitor. Wi-Fi Alliance se află și în spatele *accesului protejat Wi-Fi* (în limba engleză: *Wi-Fi Protected Access* — acronim *WPA*), piatra de hotar dintre mult criticatul WEP și standardul de securitate 802.11i.

Wi-Fi Alliance are trei scopuri principale:

- Promovarea certificării Wi-Fi în întreaga lume, prin încurajarea producătorilor în direcția utilizării proceselor standardizate 802.11 la dezvoltarea produselor pentru LAN-uri fără fir.
- Lansarea produselor certificate Wi-Fi pentru consumatorii de pe piețele de produse pentru locuințe, pentru firme mici și pentru firme mari.
- Testarea și certificarea interoperabilității produselor Wi-Fi.

Ce înseamnă certificarea Wi-Fi

Certificarea Wi-Fi este un proces care asigură interoperabilitatea dintre echipamentele LAN fără fir 802.11, incluzând punctele de acces și plăcile radio care se conformează unei varietăți de factori de formă. Pentru a se califica pentru obținerea certificării Wi-Fi, o companie trebuie să devină membră a Wi-Fi Alliance.

Wi-Fi Alliance urmărește un program de testare consacrat pentru a certifica faptul că produsele sunt interoperabile cu alte produse certificate Wi-Fi. După ce un produs trece cu succes prin fiecare test, producătorului îi este recunoscut dreptul de a folosi logo-ul „Wi-Fi Certified” (certificat Wi-Fi) pe respectivul produs și pe ambalajul și documentația aferente acestuia.

Certificarea Wi-Fi este destinată să ofere clienților încredere că achiziționează produse LAN fără fir care întrunesc cerințele de interoperabilitate ale mai multor producători. Prezența logo-ului Wi-Fi pe un produs înseamnă că acesta corespunde cerințelor testelor de interoperabilitate și va putea, cu certitudine, să conlucreze cu produsele certificate Wi-Fi ale altor producători.

Accesul protejat Wi-Fi

Criptarea WEP 802.11 nu oferă protecție suficientă pentru cele mai multe dintre aplicațiile LAN fără fir de întreținere. Datorită utilizării unei chei statice, codul WEP este destul de ușor de spart folosind instrumente care se pot achiziționa din magazine. Acest lucru îi motivează pe managerii IT să folosească forme mai puternice și mai dinamice de WEP.

Însă, problema este că aceste mecanisme pentru protecție sporită sunt brevetate, ceea ce le face să accepte cu dificultate dispozitivele client realizate de mai mulți producători. Prin urmare, Wi-Fi Alliance a făcut un important pas înainte în direcția grăbirii standardizării eficiente a securității LAN-urilor fără fir, prin definirea WPA, în timpul promovării interoperabilității. În cazul folosirii WPA, un mediu în care se află multe tipuri diferite de NIC-uri radio 802.11 — cum ar fi punctele fierbinți publice — poate beneficia de forme îmbunătățite de criptare.

WPA 1.0 este o etapă a versiunii inițiale, neratificate, a standardului 802.11i, care include protocolul de integritate cu cheie temporară (în limba engleză: Temporal Key Integrity Protocol — acronim TKIP) și mecanismele 802.1x. Combinația acestor două mecanisme asigură criptarea cu cheie dinamică și autentificarea mutuală, lucruri de care au nevoie LAN-urile fără fir.

Pentru autentificare, WPA 1.0 utilizează o combinație între autentificarea pentru sisteme deschise și autentificarea 802.1x. Inițial, clientul fără fir se autentifică în raport cu punctele de acces, ceea ce autorizează clientul să transmită cadre unui punct de acces. În continuare, WPA realizează autentificarea la nivelul utilizatorului pe baza 802.1x. În timpul acesteia, WPA 1.0 se conectează la un server de autentificare din rețeaua de întreținere. De asemenea, dacă nu este disponibil nici un server de autentificare extern, cum se întâmplă în cazul rețelelor pentru locuințe sau pentru sediile de firme mici, WPA 1.0 poate să funcționeze în ceea ce este cunoscut sub numele de modul cu cheie pre-partajată.

Standardul 802.11i este compatibil cu WPA1.0; însă, 802.11i include și criptarea opțională numită Advanced Encryption Standard (AES). AES necesită prezența coprocesoarelor, care nu sunt conținute astăzi în majoritatea punctelor de acces, ceea ce determină ca AES să fie mai potrivit pentru LAN-urile fără fir nou instalate. WPA 2.0, versiunea mai nouă de acces protejat Wi-Fi, include AES.

HiperLAN/2

HiperLAN/2, care provine de la High Performance Radio LAN (LAN radio de înaltă performanță), este un standard LAN fără fir dezvoltat de către Broadband Radio Access Networks (BRAN), o secție a Institutului pentru Standarde de Telecomunicații Europene (în limba engleză: European Telecommunications Standards Institute — acronim ETSI). HiperLAN/2 definește o tehnică LAN fără fir eficientă, de mare viteză de transmisie, care satisface în întregime cerințele reglementărilor europene de spectru.

HiperLAN/2 are un strat fizic similar cu cel al IEEE 802.11a, care funcționează cu viteze de până la 54 Mbps, în banda de 5 GHz, folosind OFDM. O deosebire majoră a standardului HiperLAN/2 față de IEEE 802.11a, constă în aceea că utilizează un protocol orientat pe conexiune și multiplexarea cu divizarea timpului (în limba engleză: time division multiplexing — acronim TDM) ca baze pentru realizarea transferului de date între utilizatori. Această metodă de transmisie este eficientă pentru aplicațiile multimedia incluzând transmisiile video și transmisiile de voce.

Îmbunătățirile aduse de HiperLAN/2

Asemănările dintre 802.11a și HiperLAN/2 se opresc, însă, la nivelul stratului MAC. În timp ce rețelele 802.11a folosesc CSMA/CA pentru a transmite pachetele de date, HiperLAN/2 utilizează *accesul multiplu prin divizarea timpului* (în limba engleză: *Time Division Multiple Access* — acronim TDMA). O problemă legată de CSMA/CA este că acesta face ca stațiile să aștepte o perioadă nedefinită de timp, ceea ce se numește acces asincron. În cazul acestui mod de operare, nu există nici un fel de relații regulate de timp asociate cu accesul la mediu. Prin urmare, nu există vreo garanție privitoare la momentul în care o anumită stație va putea să transmită un pachet. Lipsa unui acces regulat la mediu scade eficiența sistemului, lucru care nu este bun pentru asigurarea transmisiilor informațiilor video sau de voce.

Utilizarea TDMA în rețelele HiperLAN/2 oferă, însă, o relație regulată de timp pentru accesul la rețea. Sistemele TDMA atribuie în mod dinamic fiecărei stații o fereastră de timp bazată pe necesitățile de transfer (în limba engleză: throughput) ale stației. Apoi, stațiile transmit la intervale regulate, pe perioada unei ferestre de timp, făcând astfel ca mediul să fie utilizat mai eficient și îmbunătățind asistența acordată aplicațiilor video sau de voce.

HiperLAN/2 posedă un număr de caracteristici atractive prin comparație cu 802.11. Prima, și probabil și cea mai importantă, este transferul de informații mai ridicat. Atât 802.11a, cât și HiperLAN/2, realizează viteze de transmisie maxime de 54 Mbps, dar acestea nu reprezintă viteza efectivă de transfer a informațiilor între stație și punctul de acces.

Transferul maxim utilizabil, real, al unei rețele HiperLAN/2 este de 42 Mbps, în vreme ce transferul maxim utilizabil al unei rețele 802.11a este de numai aproximativ, 18 Mbps. Acest lucru face ca sistemele HiperLAN/2 să se afle mult în fața sistemelor 802.11a, în ceea ce privește performanțele fiecărui punct de acces.

O particularitate unică a tehnicii HiperLAN/2 este capacitatea de a realiza o interfață cu alte rețele de mare viteză, incluzând rețelele de telefonie celulară din generația a treia (3G), rețelele cu mod de transfer asincron (ATM) și alte rețele bazate pe protocolul Internet. Acest lucru poate constitui un avantaj real atunci când LAN-uri fără fir sunt integrate cu sistemele celulare și cu WAN-urile.

Constituie sistemele HiperLAN/2 o amenințare pentru sistemele 802.11?

În ciuda predicțiilor îndrăznețe privitoare la producția de masă și la instalarea de produse HiperLAN/2 în cursul celei de a doua jumătăți a anului 2002, nu există, în mod curent, multe produse HiperLAN/2 disponibile pentru a fi achiziționate de către consumatori. De fapt, căutări exhaustive pe Internet nu au scos la iveală nici un produs HiperLAN/2 disponibil pentru consumatori. HiperLAN/2 nu pare a câștiga teren într-un ritm sesizabil.

În mare măsură, acest lucru se petrece datorită problemelor legate de reglementare și datorită îndepărtării unor suporteri importanți de mișcarea HiperLAN/2. În plus, grupul de lucru 802.11h lucrează la revizuirea standardelor 802.11 care le vor face mai potrivite pentru a fi implementate în Europa, care este locul unde HiperLAN/2 ar putea să domine piața, dacă va ajunge să facă acest lucru undeva.

În esență, standardul 802.11h este standardul 802.11a la care se adaugă două caracteristici europene. Prima dintre acestea este controlul puterii de transmisie (în limba engleză: Transmit Power Control — acronim TPC), care permite controlul automat pentru menținerea transmisiilor în afara interferențelor cu alte sisteme învecinate. A doua caracteristică este selectarea dinamică a frecvenței (în limba



engleză: Dynamic Frequency Selection — acronim DFS), care permite stației să asculte mediul aerian înainte de a alege un canal de transmisie. Acesta este, de asemenea, un mecanism de evitare a interferențelor cerut de ETSI pentru funcționare în Europa.

În prezent, implementările 802.11 ocupă o poziție definită de lider pe piața mondială fiind cele mai căutate soluții pentru instalarea de LAN-uri fără fir. Acest lucru face ca rețelele 802.11 să fie, în ziua de azi, singura alternativă pentru instalarea de LAN-uri fără fir. Combinată cu absența de pe piață a produselor HiperLAN/2, această situație face să fie îndoielnic faptul că HiperLAN/2 va recupera handicapul și va deveni un jucător dominant pe piața LAN-urilor fără fir.

Rezumatul capitolului

Componentele LAN fără fir includ NIC-uri radio, puncte de acces, routere, repetitoare și antene, care permit realizarea de aplicații fără fir în clădiri și în complexe de clădiri (campusuri). Aceste componente sunt cărămizile care servesc la construirea implementărilor de LAN-uri fără fir în locuințe, sedii de firme mici, întreprinderi și „puncte fierbinți” publice. Aceste rețele pot cuprinde de la un singur punct de acces, pentru o locuință sau pentru un sediu mic, până la sute de puncte de acces pentru a acoperi o clădire mare (sau un complex de clădiri). Sau, LAN-ul fără fir poate fi format din numai doi utilizatori care comunică direct unul cu celălalt, folosind modul ad-hoc.

802.11 este, de departe, cel mai important standard la nivel mondial, asigurând viteze de transmisie a datelor de până la 54 Mbps și funcționând fie în banda de frecvențe de 2,4 GHz, fie în cea de 5 GHz. Wi-Fi oferă asigurări cu privire la interoperabilitatea dintre componentele LAN fără fir care se conformează standardului 802.11 dar sunt fabricate de producători diferiți, iar HiperLAN/2 este un standard bazat pe cerințele europene care este improbabil că va constitui un competitor serios pentru 802.11.

Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. Care este componenta LAN fără fir cel mai des folosită în locuințe și în sediile firmelor mici?
2. Care este principala diferență dintre un punct de acces și un router LAN fără fir?
3. Când are sens să fie utilizat un repetor LAN fără fir?
4. Cum identifică o placă NIC radio pentru LAN-uri fără fir punctul de acces cu care să se asocieze?
5. WEP este un mecanism de criptare obligatoriu. Adevărat sau fals?
6. Care este banda de frecvență în care funcționează rețelele 802.11a?
7. Câte canale de transmisie, care nu se suprapun, sunt disponibile într-o rețea LAN fără fir 802.11b?
8. Adevărat sau fals: rețelele 802.11g funcționează la viteze de transmisie a datelor de până la 54 Mbps și sunt interoperabile cu rețelele 802.11b.
9. Care dintre frecvențele specificate de standardul 802.11 este disponibilă aproape oriunde în lume?
10. Ce oferă certificarea Wi-Fi?

engleză: Dynamic Frequency
asculte mediul aerian înainte
asemenea, un mecanism
în Europa.

În prezent, im
mondială fiind c
lucru face ca
instalarea d
HiperLAN
handica

A. intitulată Răspunsuri

AN fără fir?

es cu

lor fără fir;

ehnicile utilizate de aceste

... fără fir.

CAPITOLUL 6

MAN-urile fără fir: rețele pentru conectarea clădirilor și a locațiilor aflate la distanță

MAN-urile fără fir satisfac necesitățile de conectare în rețea pe suprafața unui oraș sau a unei zone rurale. În general, MAN-urile fără fir realizează interconectarea utilizatorilor staționari. În cele mai multe cazuri, MAN-urile fără fir oferă conexiuni exterioare staționare.

MAN-urile fără fir conduc la un profit mare în urma investiției, deoarece companiile evită închirierea sau instalarea unor legături costisitoare bazate pe cabluri cu fire de cupru sau pe cabluri optice. De fapt, uneori este imposibil să instalați o rețea cu fir între două puncte, atunci când restricțiile legale fac ca instalarea cablurilor să fie prohibitivă. De exemplu, o companie poate utiliza componente MAN fără fir pentru comunicațiile de date dintre sediul central al firmei și un centru de distribuție învecinat.

În multe cazuri, companiile pot realiza suficiente economii, ca urmare a folosirii unei rețele MAN fără fir, pentru a-și recupera investiția făcută într-un an sau doi. Acest lucru încurajează, cu siguranță, orice companie care are nevoie să stabilească comunicații între clădiri răspândite pe suprafața unui oraș, să utilizeze o rețea MAN fără fir.

Acest capitol oferă exemple de componente MAN fără fir, descrie modul în care aceste componente sunt interconectate pentru a forma o varietate de sisteme și explorează diversele standarde.

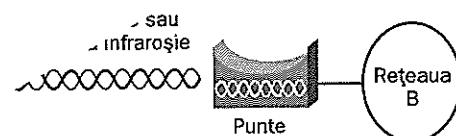
engleză: Dynamic Frequency
asculte mediul aerian înair
asemenea, un mecanism
în Europa.

În prezent, im
mondială fiind c
lucru face ca
instalarea d
HiperLAN
handica

A. intitulată Răspunsuri
și în sedile
AN fără fir?

general, în perechi potrivite,
unct la un altul. Să aruncăm
AN fără fir.

tează două rețele
'ate (stratul 2 al



fir sunt plasate, de regulă, la fiecare capăt al legăturii punct la punct,
cea care interconectează două clădiri. O punte are un port pentru fir care o
conectează la rețea și un port fără fir care asigură interfața cu un transceiver. Puntea
primește pachete prin unul dintre porturi și le retransmite prin celălalt. O punte nu va
începe o retransmisie până când nu recepționează un pachet complet. De aceea,
stațiile aflate de fiecare parte a punții pot transmite pachete simultan, fără a se
produce coliziuni.

Unele punți retransmit orice pachet prin portul opus, indiferent dacă pachetul
respectiv este destinat unei stații aflate în rețeaua din partea cealaltă. O punte care
învață, un tip mai des utilizat, examinează adresa de destinație a fiecărui pachet
pentru a stabili dacă va retransmite pachetul pe baza unui tabel de decizie pe care
puntea îl construiește în timp. Acest lucru crește eficiența, deoarece puntea nu va
retransmite un pachet dacă știe că adresa de destinație a acestuia este pe aceeași parte
a punții unde se află și adresa sursei. De asemenea, punțile care învață actualizează
înregistrările din tabelul de adrese, eliminând acele adrese care au fost inactive o
anumită perioadă de timp.

Punțile dintr-o rețea sunt transparente pentru utilizator, în sensul că pachetele
sunt transmise prin punte în mod automat. De fapt, utilizatorii nu sesizează că
pachetele lor traversează o legătură care le conduce la o altă locație.

Punți contra puncte de acces

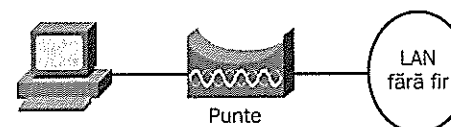
Punctele de acces conectează fără fir mai mulți utilizatori la o rețea cu fir și între
ei. De exemplu, câțiva utilizatori echipați cu NIC-uri 802.11 se pot asocia la un
singur punct de acces care îi conectează la o rețea Ethernet. Fiecare utilizator are
acces la rețeaua Ethernet și la toți ceilalți utilizatori. În acest caz, punctul de acces
este similar cu un dispozitiv punte, însă punctul de acces realizează interfețele unei
rețele cu mai mulți utilizatori. O punte realizează doar interfețe cu alte rețele.

Există posibilitatea utilizării unei punți fără fir pentru aplicații de interior. De
exemplu, o punte LAN fără fir poate conecta o rețea Ethernet direct la un anumit
punct de acces. Acest lucru poate fi necesar atunci când câteva dispozitive, posibil
aflate într-o parte îndepărtată a clădirii, sunt interconectate printr-o rețea Ethernet. O
punte LAN fără fir este atașată fizic la această rețea Ethernet și utilizează protocolul
802.11 pentru a comunica cu un punct de acces care se află în raza sa de acțiune. În
acest fel, puntea asigură conectarea fără fir a unui grup de utilizatori (de fapt o rețea)
la un punct de acces.

Punți de bază pentru conectare Ethernet-la-rețea-fără-fir

O punte Ethernet-la-rețea-fără-fir (vezi figura 6.2) este conectată direct la un
dispozitiv de calcul printr-un port Ethernet și apoi furnizează o conexiune fără fir la
un punct de acces. Acest lucru face ca puntea să fie utilă atunci când dispozitivul
(care poate fi o imprimantă, un PC sau o consolă pentru jocuri video) are un port
Ethernet și nu posedă o placă NIC fără fir. În unele cazuri, s-ar putea să nu existe
posibilitatea atașării unei plăci NIC fără fir, ceea ce face ca o punte de bază să fie
singura modalitate de realizare a unei comunicări fără fir. Imprimantele și mașinile
pentru jocuri video sunt exemple comune ale unui astfel de scenariu.

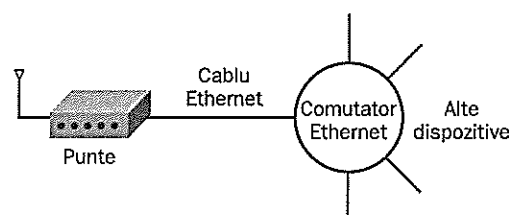
Figura 6.2. O punte de bază conectează un PC la o rețea LAN fără fir



Punți grup de lucru

Punțile grup de lucru (în limba engleză: workgroup bridges) constituie soluția pentru conectarea rețelelor fără fir la rețele Ethernet (cu fir) mai extinse. O punte grup de lucru se comportă ca un client conectat fără fir, dintr-o rețea fără fir, care se conectează la o rețea cu fir. Partea cu fir a punții este conectată la un comutator Ethernet care asigură legătura cu mai multe dispozitive. O punte grup de lucru oferă utilități de securitate mai solide și un management de nivel superior al transmisiei — la un preț mai ridicat — prin comparație cu o punte de bază.

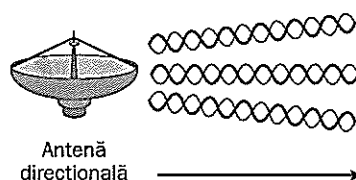
Figura 6.3. O punte grup de lucru asigură conectarea la rețelele cu fir standard



Antene direcționale

O antenă este un element important al unei MAN fără fir. Spre deosebire de alte tipuri de rețele fără fir, majoritatea antenelor utilizate de MAN-urile fără fir sunt *antene direcționale*, în special pentru că acestea operează pe distanțe mai mari. Figura 6.4 ilustrează propagarea undelor radio pornite de la o antenă direcțională. Acest mod de propagare se deosebește de cel produs de o antenă omnidirecțională, care transmite unde radio în toate direcțiile.

Figura 6.4. Antenele direcționale maximizează intensitatea undelor radio pe o singură direcție



Diferitele tipuri de antene au diferite lățimi de lob (în limba engleză: beamwidth) pe verticală și pe orizontală. De exemplu, o antenă omnidirecțională are o lățime de lob orizontală de 360 de grade și o lățime de lob verticală cuprinsă între 7 și 80 de

grade. O antenă semidirecțională poate avea o lățime de lob verticală de 20 de grade și una orizontală de 50 de grade. În general, cu cât lățimea de lob este mai îngustă, cu atât crește distanța pe care puterea transmisă este menținută constantă.

Antene semidirecționale

Există câteva tipuri de antene care au moduri de radiație semidirecționale. De exemplu, o antenă cu fâșie direcțională (în limba engleză: directional patch antenna) va avea o rază de acțiune cel puțin dublă față de o antenă omnidirecțională. Puteți monta cu ușurință o astfel de antenă pe un perete exterior al clădirii și astfel veți acoperi eficient o distanță mare. O antenă Yagi (tip comun de antenă inventat de japonezul Hidetsugu Yagi) este cea mai bună antenă semidirecțională pentru aplicațiile la mare distanță.

Antenele semidirecționale realizează o creștere eficientă a amplitudinii semnalului — cunoscută sub numele de câștig — de aproximativ 10 ori. Aceste antene sunt utilizate mai ales pentru a extinde LAN-urile fără fir în scopul acoperirii de suprafețe mai mari. De exemplu, o universitate poate instala o antenă Yagi pentru a realiza o acoperire eficientă a suprafeței exterioare, deschise și întinse a unui campus. MAN-urile fără fir acoperă, în general, distanțe mult mai mari și necesită valori mai mari ale câștigului.

Antene de mare directivitate

O antenă de mare directivitate are o lățime de lob extrem de îngustă, cu modele de radiație lungi și o rază de acțiune corespunzătoare. Pentru a realiza acest grad de directivitate, va trebui să utilizați antene parabolice care concentrează energia undelor radio mai ales într-o anumită direcție. Aceste tipuri de antene sunt scumpe prin comparație cu cele omni sau semidirecționale; însă, costurile pot fi acceptabile, dacă soluția cere o rază mare de acțiune.

Multe dintre antenele direcționale de mare câștig sunt antene parabolice care concentrează puterea semnalului de radio frecvență (RF) într-o singură direcție. O antenă parabolică, de exemplu, are o lățime de lob orizontal și vertical cuprinsă între 4 și 25 de grade. Această concentrare extremă a puterii semnalului RF sporește considerabil raza de acțiune.

Însă, o problemă legată de antenele parabolice este aceea că pot fi distruse de intemperii datorită solicitării excesive produse de către vânt, mai ales dacă antena nu este montată corect. Prin urmare, antenele grilă de mare directivitate, care posedă multe goluri pe suprafața parabolică sunt, în general, mai sigure.

În plus, atât antenele semidirecționale cât și cele de mare directivitate necesită o linie de propagare liberă între punctele de capăt ale sistemului. În unele cazuri, semnalele RF pot trece prin copaci și prin unele clădiri, însă lumina infraroșie necesită o cale de propagare lipsită de obstacole. De asemenea, semnalele RF și cele de lumină infraroșie sunt atenuate periodic datorită obstacolelor în mișcare care intersectează calea de propagare, cum ar fi trenurile și automobilele aflate în mers. Proiectarea MAN-urilor fără fir este dificilă în mediile citadine din cauza clădirilor care blochează calea de propagare dintre punctele de capăt ale sistemului.

Efectul de polarizare

Polarizarea antenei este o orientare fizică a acesteia pe un plan orizontal sau vertical. De exemplu, polarizarea verticală, care este cea mai comună la LAN-urile fără fir, apare atunci când antena este perpendiculară pe suprafața Pământului. Polarizația paralelă caracterizează o antenă care este orientată paralel cu suprafața Pământului.

Pentru a maximiza transferul energiei RF de la antena emițătoare la cea receptoare, ambele trebuie să aibă aceeași polarizație. Dacă o antenă are polarizare verticală, iar cealaltă polarizare orizontală, nu se produce transferul puterii semnalului de comunicație.

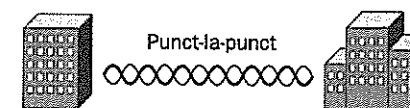
Sisteme MAN fără fir

MAN-urile fără fir oferă conexiuni între clădirile și utilizatorii de pe aria unui oraș sau a unui campus prin intermediul câtorva configurații de sistem. În majoritatea cazurilor, MAN-urile fără fir folosesc undele RF sau lumina infraroșie pentru a transmite semnalele de la un punct la altul cu ajutorul antenelor direcționale.

Sisteme punct-la-punct

O soluție punct-la-punct folosește semnale RF sau semnale de lumină infraroșie emise fie de antene semidirecționale fie de antene de mare directivitate pentru a extinde raza de acțiune pe suprafața unui oraș sau a unui campus. Raza de acțiune poate fi de până la 50 de kilometri pentru sistemele RF care utilizează antene de mare directivitate. Figura 6.5 ilustrează un sistem MAN fără fir punct-la-punct.

Figura 6.5. O rețea MAN fără fir punct-la-punct conectează două puncte ale rețelei

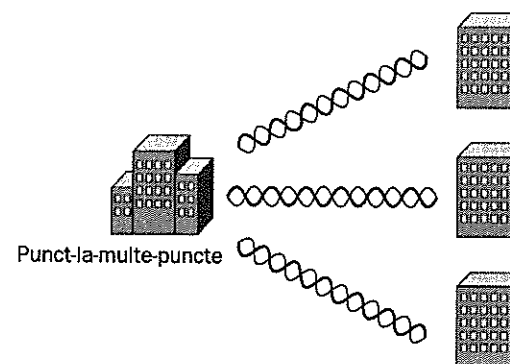


De exemplu, un centru medical poate utiliza o MAN fără fir punct-la-punct pentru a asigura o legătură de comunicații între sediul central al spitalului și clinici aflate la distanță de acesta, în același oraș. Sistemul care rezultă nu asigură, însă, o flexibilitate comparabilă cu cea oferită de soluțiile punct-la-multe-puncte. Totuși, dacă există doar necesitatea conectării unei perechi de locații, costul implementării unui **sistem punct-la-punct** este mai scăzut prin comparație cu cel al implementării unui sistem punct-la-multe-puncte.

Sisteme punct-la-multe-puncte

O legătură tipică punct-la-multe-puncte (vezi figura 6.6) utilizează o antenă omnidirecțională centrală care folosește un singur transceiver pentru a asigura legătura cu mai multe stații aflate la distanță. De exemplu, o clădire din centrul unui oraș poate găzdui o antenă omnidirecțională, iar alte clădiri aflate pe raza orașului respectiv pot avea antene direcționale îndreptate către locația centrală. Transceiverul central recepționează și retransmite semnalele.

Figura 6.6. O rețea MAN fără fir punct-la-multe-puncte interconectează utilizatorii prin intermediul unui transceiver central comun

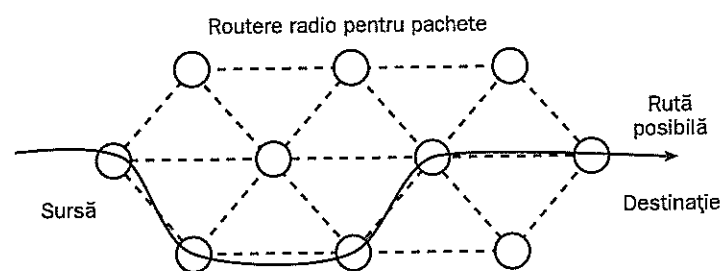


Un avantaj important al unui MAN fără fir punct-la-multe-puncte este acela că sistemul face ca adăugarea de noi conexiuni să fie ușor de realizat. De fapt, această abordare poate fi mai ieftină prin comparație cu sistemele punct-la-punct atunci când există mai multe locații care trebuie interconectate sau conectate la o locație centrală. De exemplu, sediul central al unei companii care deține mai multe depozite și fabrici în același oraș sau în aceeași zonă rurală poate beneficia de pe urma folosirii unui *sistem punct-la-multe-puncte*.

Sisteme radio cu pachete de date

Un sistem radio cu pachete (vezi figura 6.7) utilizează routere fără fir speciale, care retransmit la destinație pachete de date. Fiecare utilizator are o NIC pentru pachete radio care transmite datele celui mai apropiat router fără fir. Apoi, acest router retransmite datele routerului următor. Aceste salturi de la un router la altul au loc până când pachetul de date ajunge la destinație. Acest tip de rețea cu ochiuri nu este nou. Radioamatorii îl folosesc de decenii, iar companii cum ar fi Metricom, au instalat acest tip de sistem, în orașele mari, de aproape 10 ani.

Figura 6.7. Sistemele radio cu pachete transferă pachetele de date, prin salturi repetate, de la sursă până la destinație



Administrația unui oraș poate dori să desfășoare un sistem radio cu pachete pentru a oferi conectivitatea fără fir în scopul realizării unor aplicații pe aria întregului oraș. Instalarea de routere în locuri strategice din oraș furnizează infrastructura necesară. Nu sunt necesare cabluri pentru interconectarea routerelor. Fiecare router poate recepționa și retransmite pachetele până ce acestea ajung la destinație.

Totodată, acest tip de rețea funcționează și dacă unele routere nu mai sunt operaționale. Dacă unul dintre routere nu mai funcționează, din cauza unui trăsnet sau a unui sabotaj, protocoalele de direcționare adaptative actualizează, în mod automat, tabelul de direcționare al fiecărui router astfel încât pachetele de date vor evita să treacă prin routerul nefuncțional.

Tehnici MAN fără fir

Multe dintre sistemele MAN fără fir utilizează tehnici brevetate care funcționează în benzi de frecvență care necesită licență. Licențierea evită potențialele interferențe RF, asigurând utilizarea de frecvențe diferite de funcționare pentru sistemele învecinate. Chiar dacă utilizatorii finali trec printr-un proces de obținere a licenței, nu se pierde mult timp deoarece licențierea se face o singură dată. Însă, apare o problemă legată de faptul că acele componente care lucrează în benzile licențiate sunt scumpe.

Prin urmare, companiile preferă să folosească echipamente bazate pe standarde, ceea ce conduce, în general, la costuri mai mici, atât pentru instalare, cât și pentru întreținere. Dacă producătorul nu mai asigură asistență pentru un anumit produs, compania poate apela la un alt producător atunci când modifică rețeaua. Standardele sporesc, cu certitudine, longevitatea sistemului.

802.11 și Wi-Fi

Multe companii instalează MAN-uri fără fir utilizând standarde LAN fără fir, cum ar fi 802.11 și Wi-Fi. Capitolul 5, intitulat *LAN-urile fără fir: rețele pentru clădiri și complexe de clădiri*, oferă detaliile privitoare la aceste standarde. Diferența constă în faptul că MAN-urile fără fir folosesc antene direcționale pentru a stabili o legătură punct-la-punct între punctele fixe ale sistemului. Hardware-ul utilizat include o punte fără fir care implementează standardele LAN fără fir.

Utilizarea de hardware LAN fără fir pentru rețele de dimensiunile unui oraș conduce la scăderea costurilor, însă, rețelele 802.11 au performanțe limitate atunci când asigură conectarea unui număr mare de utilizatori care au nevoie de o lărgime de bandă garantată. În plus, interferențele RF constituie adesea o problemă semnificativă a

rețelor 802.11 atunci când acestea acoperă arii mari, datorită funcționării libere de licență. Un competitor poate instala o rețea 802.11 care să producă interferențe cu rețeaua dumneavoastră, iar utilizatorii vor avea de suportat o scădere sporadică a performanțelor. Această problemă nu are soluție, deoarece nu există un fundament legal pentru remedierea situației.

802.16

Grupul IEEE 802 a inițiat grupul de lucru IEEE 802.16 pentru a crea standarde pentru accesul fără fir de bandă largă, care să ofere o soluție accesibilă, cu costuri reduse, de mare capacitate și de mare viteză, pentru extinderea magistralelor de fibră optică. Primul standard IEEE **802.16**, publicat în aprilie 2002, definește interfața aeriană MAN fără fir (în limba engleză: Wireless MAN Air Interface) pentru rețelele MAN fără fir. Aceste sisteme sunt destinate să furnizeze acces la rețea pentru locuințe, firme mici și clădiri comerciale, ca o alternativă la conexiunile tradiționale cu fir.

Cu un echipament pentru stațiile de bază fără fir proiectat la un cost sub 20 000 \$, o rețea 802.16 poate deservi economic până la 60 de clienți prin conexiuni de viteză T-1 (1,5 Mbps). Acest lucru este atractiv pentru un furnizor de servicii Internet fără fir (WISP) tipic, care nu dispune de sume mari pentru investiții. În plus, rețeaua 802.16 poate oferi o posibilitate avantajoasă de a conecta laolaltă puncte fierbinți dotate cu LAN-uri fără fir.

Standardul 802.16 permite implementarea arhitecturii punct-la-multe-puncte în domeniul de frecvență 10-66 GHz, transmițând date la viteze de până la 120 Mbps. La aceste frecvențe, transmisia necesită o cale de propagare dreaptă și liberă, iar acoperișurile oferă cele mai bune locații pentru montarea stației de bază și a stațiilor de abonați. Stația de bază se conectează la o magistrală cu fir/fibră și poate transmite fără fir la distanțe de până la 50 de kilometri către un mare număr de stații staționare de abonat, posibil sute.

Pentru a rezolva problema accesului la rețea, la frecvențe mai joase, a locațiilor care nu au între ele o linie de propagare dreaptă fără obstacole, IEEE a publicat în ianuarie 2003 standardul 802.16a, care asigură suportul pentru arhitectură celulară (rețeaua cu ochiuri). Rețelele 802.16a funcționează în frecvențe licențiate și nelicențiate cuprinse între 2 GHz și 11 GHz, folosind multiplexarea prin divizarea ortogonală a frecvenței (OFDM).

Stratul MAC 802.16 suportă multe specificații diferite pentru stratul fizic, atât licențiate cât și nelicențiate. Prin intermediul stratului MAC 802.16, fiecare stație de bază distribuie dinamic stațiilor abonate lărgimi de bandă pentru emisie și pentru recepție folosind accesul multiplu prin divizarea timpului (TDMA). Aceasta constituie o diferență foarte importantă prin comparație cu stratul MAC 802.11, la care implementările curente funcționează utilizând mecanisme de sesizare a purtătoarei care nu oferă un control eficace al lărgimii de bandă asigurate prin legătura radio.

Următorul pas pe care urmează să-l facă grupul de lucru IEEE 802.16 este să adauge standardului portabilitate și mobilitate. În martie 2002, a început grupul de studiu 802.16e pentru accesul fără fir, de bandă largă, mobil (în limba engleză: Mobile Broadband Wireless Access). Acest grup va ataca multe aspecte diferite privitoare la mobilitate, incluzând asigurarea conectivității pentru vehicule aflate în mișcare, în sectorul unei stații de bază.

Rezumatul capitolului

MAN-urile fără fir folosesc, în primul rând, punți cu antene direcționale pentru a interconecta două sau mai multe rețele aflate pe suprafața unui oraș. Sistemele punct-la-punct conectează direct două locații, iar sistemele punct-la-multe-puncte permit ca mai multe locații să se conecteze la un transceiver central. Multe firme utilizează tehnici brevetate pentru MAN-urile fără fir. Standarde cum sunt 802.11 și Wi-Fi permit realizarea de soluții mai ieftine, însă persistă posibilitatea apariției interferențelor RF. Standardul 802.16, promite, însă, să ofere soluții pentru realizarea de MAN-uri fără fir eficiente, bazate pe standarde.

Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. De ce instalarea MAN-urilor fără fir asigură beneficii bune în urma investiției?
2. O punte care învață retransmite toate pachetele primite. Adevărat sau fals?
3. Care este diferența principală dintre o punte și un punct de acces?
4. Care sunt exemplele de antene semidirecționale prezentate în acest capitol?
5. Care este diferența principală dintre o antenă semidirecțională și una de mare directivitate, din punctul de vedere al lății de lob?
6. Dați un exemplu de antenă de mare directivitate.
7. Care este cea mai eficace polarizare a unei antene receptor, dacă emițătorul folosește polarizarea verticală?
8. Care sunt avantajele utilizării unui sistem punct-la-multe-puncte, prin comparație cu sistemele punct-la-punct, în cazul interconectării mai multor locații?
9. Care sunt avantajele utilizării sistemelor radio cu pachete pentru MAN-urile fără fir?
10. Care sunt standardele folosite de MAN-urile fără fir?

Ce veți învăța

După citirea acestui capitol, veți putea:

- ✓ să recunoașteți aplicațiile specifice ale WAN-urilor fără fir;
- ✓ să înțelegeți componentele și standardele utilizate de WAN-urile fără fir;
- ✓ să înțelegeți bine diversele tipuri de sisteme WAN fără fir.



WAN-uri fără fir: rețele pentru conexiuni pe tot globul

WAN-urile fără fir satisfac necesitățile de conectare la distanțe mari, de dimensiunile țărilor sau continentelor. În majoritatea cazurilor, WAN-urile fără fir oferă conexiuni la distanțe mari față de casă, de birou și de LAN-urile fără fir publice. WAN-urile fără fir asigură acoperire în interiorul clădirilor, însă performanțele realizate în aceste zone sunt adesea mai scăzute decât în cazul funcționării în exterior.

Avantajul WAN-urilor fără fir este aria largă de acoperire și costurile scăzute per utilizator. Dezavantajul provine din disponibilitatea limitată a spectrului de frecvență, care conduce la performanțe scăzute și la o securitate limitată. Totuși, WAN-urile fără fir sunt mai economice decât LAN-urile fără fir atunci când sunt desfășurate pe spații largi. O performanță limitată este mai bună decât deloc.

De exemplu, o rețea WAN fără fir permite cuiva să-și verifice e-mail-ul prin intermediul unui PDA, în timp ce vizitează un client dintr-un alt oraș. Acest lucru permite utilizatorului să acționeze mai rapid în anumite situații, decât în cazul în care ar aștepta să ajungă în camera sa de hotel pentru a-și verifica e-mail-ul. Performanța relativ scăzută a rețelei extinse fără fir oferă un suport adecvat pentru acest tip de aplicație.

WAN-urile fără fir pot furniza și accesul la Internet de la o locație staționară. De exemplu, un vilegiaturist poate să poziționeze corespunzător o antenă de satelit montată pe vehiculul său pentru recreere și să obțină astfel acces la Internet. Acest lucru face ca persoana respectivă să poată păstra contactul cu familia și să se bucure de beneficiile Web-ului, pe timpul staționării în zone îndepărtate.

Capitolul acesta oferă exemple de componente WAN fără fir, descrie modul în care aceste componente sunt interconectate pentru a forma o varietate de sisteme și explorează diversele tehnici WAN fără fir.



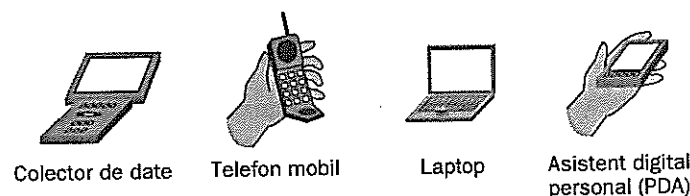
Componente WAN fără fir

WAN-urile fără fir satisfac atât necesitățile aplicațiilor staționare cât și pe cele ale aplicațiilor mobile. În consecință, componentele sunt diferite în funcție de tehnicile și de configurațiile WAN-urilor fără fir. De exemplu, o rețea WAN fără fir bazată pe satelit are componente diferite față de un sistem celular.

Dispozitive pentru utilizatorii de WAN-uri fără fir

Utilizatorii WAN-urilor fără fir folosesc dispozitive portabile, de mici dimensiuni. Aceasta deoarece accesul la rețea este disponibil pe suprafețe mult mai mari, iar utilizatorii trebuie să-și poarte dispozitivele cu ei. De exemplu, o persoană care călătorește pentru afaceri poate purta cu ea un mic PDA sau un telefon mobil prin care să acceseze e-mail-ul atunci când călătorește într-un taxi, de la aeroport la hotel. Figura 7.1 ilustrează cele mai comune tipuri de dispozitive pentru utilizatorii de WAN-uri fără fir.

Figura 7.1. Dispozitivele pentru utilizatorii de WAN-uri fără fir sunt de mici dimensiuni pentru a permite cu ușurință mobilitatea acestora



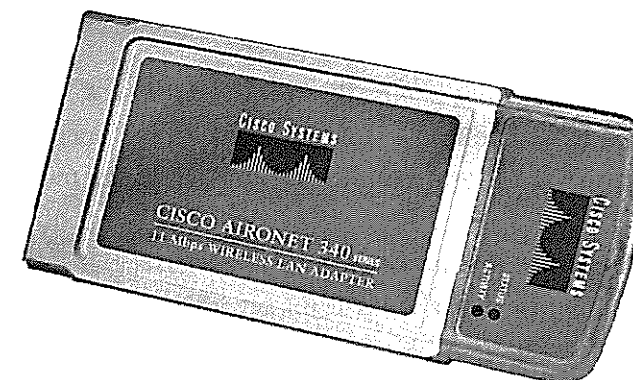
Utilizarea WAN-urilor fără fir de către PC-urile legate în rețea nu este ceva obișnuit; există totuși câteva astfel de aplicații. Nevoia de a aranja un punct de vânzare (în limba engleză: point-of-sale — acronim POS) portabil, aflat într-o zonă îndepărtată, cum ar fi o locație provizorie pentru un concert, poate îndemna la utilizarea unei WAN fără fir. Un comerciant care vinde tricouri poate procesa cărțile de credit prin intermediul unei WAN fără fir la un centru de procesare bazat pe Internet.

NIC-uri radio

Unele telefoane mobile au încorporate NIC-uri radio WAN fără fir. Companiile de telecomunicații, cum sunt Verizon și Sprint, oferă conexiuni WAN fără fir împreună cu serviciile de voce. Problema este, însă, că există câteva tipuri diferite de WAN-uri fără fir, ceea ce face ca găsirea de către utilizatori a telefonului mobil care să aibă o interfață cu tipul de WAN fără fir pe care doresc să-l folosească să constituie o provocare.

Pentru a realiza o interfață între un laptop sau un PDA și o WAN fără fir, va trebui să achiziționați o NIC radio adecvată pentru o WAN fără fir. Figura 7.2 prezintă o NIC radio disponibilă pentru WAN-uri fără fir. Aceste plăci pot arăta ca acelea pentru PAN-urile sau LAN-urile fără fir; însă, placa poate conține una dintre cele câteva tehnici incompatibile.

Figura 7.2. Există NIC-uri radio fără fir pentru PDA-uri și laptopuri



În general, comerciantul vinde, împreună cu hardware-ul, și accesul la serviciul pentru care placa este proiectată să ofere o interfață. Companiile de telecomunicații cheltuiesc sume importante de bani pentru a asigura spectrul de frecvență și pentru a instala hardware pe zone întinse. În consecință, toți furnizorii de rețele WAN fără fir taxează serviciile. Această situație diferă de cea a punctelor fierbinți cu LAN-uri fără fir, în care multe hoteluri și aeroporturi găsesc că este avantajos să ofere acces gratuit la Internet utilizatorilor unei LAN fără fir. Acest lucru este posibil pentru că instalarea unei rețele LAN fără fir nu necesită un capital mare.

Notă

Asigurați-vă că achiziționați o placă NIC radio pentru WAN-uri fără fir care oferă o interfață cu tipul de WAN fără fir disponibil în zonele în care aveți nevoie de serviciul respectiv. Aveți în vedere aria de acoperire, așa cum faceți în cazul unui telefon mobil, înainte de a decide ce placă NIC radio și ce serviciu veți utiliza.

În cazul în care utilizați o rețea WAN fără fir bazată pe satelit, devine necesară achiziționarea unui hardware de terminal pentru satelit. Versiunile mobile de terminale pentru satelit posedă o antenă parabolică reflectoare mică și electronică, care poate încăpea într-o geantă de dimensiuni medii. Acest tip de interfață WAN fără fir este relativ scumpă. Sunt disponibile și terminale de satelit pentru instalări permanente cum ar fi cele pentru montat pe vehicule pentru recreere sau pe vehicule proprietate personală.

Stații de bază

De regulă, stațiile de bază pentru WAN-uri fără fir sunt instalate în exteriorul clădirilor. De fapt, turnuri de celulă familiare, ca acela prezentat în figura 7.3, pot fi văzute răspândite peste tot prin orașe și regiuni rurale. În mod similar cu cazul LAN-urilor fără fir, aceste stații de bază se bazează pe fire pentru conectarea la un sistem de distribuție care asigură comutarea și o interfață cu Internetul. În majoritatea situațiilor, turnurile sunt amplasate în aer liber pentru a furniza o acoperire maximă. Totuși, unele clădiri publice de mari dimensiuni — cum ar fi mall-urile sau aeroporturile — instalează stații de bază celulare în interior pentru a face față unui număr mare de abonați.

O altă formă de stație de bază o constituie un *satelit* aflat pe orbită, care este, de fapt, un repetor aflat în cer. La sol, un utilizator își îndreaptă antena disc către satelit, iar satelitul recepționează semnalul și îl retransmite înapoi unei stații aflate la sol (vezi figura 7.4). Un avantaj important al acestei abordări este acela că este nevoie de mai puțină infrastructură la sol. Însă, problema este aceea că operatorii trebuie să cheltuiască milioane de dolari pentru a realiza un sistem cu satelit pentru traficul de date. Acest lucru conduce la sume mari de plată pentru utilizatori.

Figura 7.3. Turnurile de celulă sunt stații de bază obișnuite pentru WAN-uri fără fir

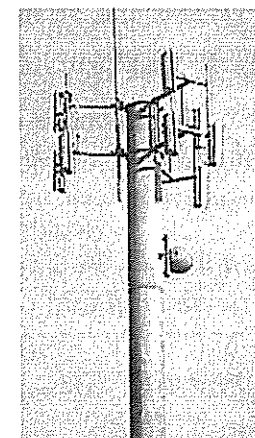
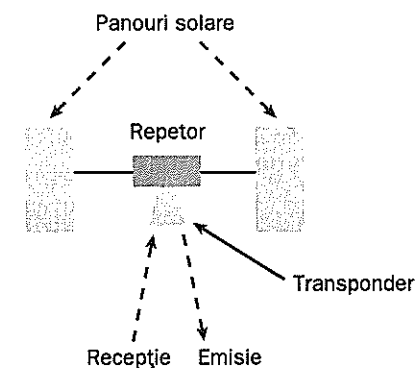


Figura 7.4. Sateliții au transpondere¹ de semnal care emit și recepționează semnale RF și celule solare care le furnizează energie electrică

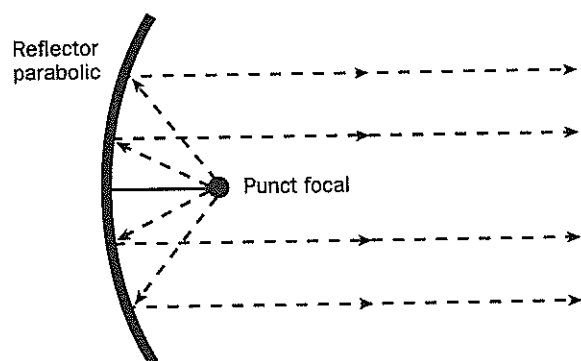
**Antene**

Stațiile de bază și dispozitivele de utilizatori pentru WAN-urile fără fir folosesc o varietate de antene în funcție de tipul de WAN fără fir. Pentru sistemele celulare, antena dispozitivelor de utilizator este, în general, omnidirecțională. Turnurile de celulă au, în general, mai multe antene direcționale care acoperă distanțe mari.

¹ Transponder sau repetor de impulsuri — în domeniul comunicațiilor prin satelit, un transmițător/receptor care primește un semnal de la o stație terestră și îl retransmite pe altă frecvență altor stații terestre (n.tr.).

Un utilizator de satelit deține o antenă parabolică având caracteristicile prezentate în figura 7.5. Transceiverul, localizat în punctul focal, transmite și recepționează semnalele de radio frecvență (RF). De exemplu, semnalele RF părăsesc emițătorul transceiverului, iar forma discului antenei le orientează într-o singură direcție.

Figura 7.5. Antenele disc au reflectoare parabolice care concentrează puterea semnalului într-un mod avantajos



Indiferent de unghiul sub care semnalele RF lovesc discul, acestea sunt reflectate într-o singură direcție datorită formei sale parabolice. De fapt, opusul este și acesta adevărat. Atunci când antena recepționează semnalele RF, forma discului le concentrează în receptorul care se află în punctul focal.

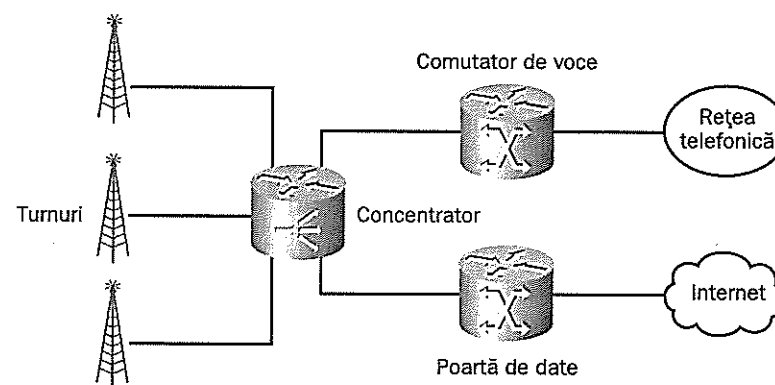
Sisteme WAN fără fir

Majoritatea WAN-urilor fără fir se bazează pe rețele celulare, însă altele folosesc sateliți. Să aruncăm o privire mai atentă asupra ambelor tipuri.

WAN-uri fără fir pe bază de rețelele celulare

Așa cum se arată în figura 7.6, un sistem celular este format din turnuri de celulă, concentratori, comutatoare de voce și porți de date. Turnurile de celulă recepționează semnalele primite de la dispozitivele utilizatorilor și transmit informații înapoi la aceștia. Un comutator de voce conectează dispozitivul utilizatorului la un alt utilizator (cu sau fără fir) prin intermediul sistemului de distribuție telefonic. Această parte a sistemului asigură convorbirile telefonice uzuale dintre utilizatori.

Figura 7.6. Sistemele celulare cuprind porți de date pentru a adăuga conexiuni de rețea fără fir la serviciile tradiționale de voce



Componenta care face ca sistemul să devină o WAN fără fir este poarta de date. În acest caz, poarta de date este capabilă să interacționeze cu protocoalele de date într-un mod care face posibil ca utilizatorii să navigheze pe Internet, să trimită și să primească mesaje e-mail și să utilizeze aplicații de corporație.

Transmiterea de mesaje text este o aplicație populară a WAN-urilor fără fir bazate pe sisteme celulare. Utilizatorii comunică prin tastarea de mesaje text scurte și prin transmiterea acestora la alți utilizatori, similar cu aplicațiile pentru transmiterea instantanee a mesajelor disponibile pentru PC-uri. Însă, în cazul dispozitivelor WAN fără fir de mai mici dimensiuni, este important ca utilizatorul să poată salva mesaje tip de genul: „Astăzi călătoresc, așa că am să vă sun mai târziu“, care pot fi transmise prin apăsarea unui singur buton. Unele dispozitive WAN fără fir captează și fotografii digitale sau secvențe video care sunt transmise prin rețea.



Prima generație de sisteme celulare

Atunci când telefoanele mobile au devenit disponibile pentru prima oară, comunicațiile fără fir utilizau numai semnale analogice. Acest sistem inițial de telefoane celulare este cunoscut sub numele de *prima generație de sisteme celulare* (în limba engleză: first-generation cellular — acronim *1G cellular*) sau *sistem 1G*. Atunci când cineva vorbește printr-un sistem 1G, vocea sa este transmisă folosindu-se modularea de frecvență (FM), care modifică numai frecvența undei purtătoare în concordanță cu semnalul audio. Sistemele 1G utilizează un număr limitat de canale care folosesc FSK pentru a transmite semnalele de control necesare pentru stabilirea și realizarea unei convorbiri.

Sistemele 1G funcționează bine pentru convorbiri telefonice, în ciuda unor trosnete și pocnituri ocazionale, însă nu sunt suficiente pentru transmiterea de date. Ca și în cazul vocii, semnalele analogice trebuie să reprezinte datele. Utilizatorii trebuie să realizeze o interfață între PC și sistemul celular folosind un modem care convertește semnalele digitale primite de la dispozitivul de calcul într-o formă analogică (cum ar fi FSK sau PSK), care este potrivită pentru transmisia printr-un canal de voce mic de 4 KHz. Acest lucru conduce la viteze scăzute de transmisie a datelor, de 20-30 Kbps.

Sistemele 1G nu au nici capacitatea de a asigura mecanisme de autentificare și de criptare. Canalul digital de control FSK are doar o capacitate suficientă pentru a asigura convorbirile telefonice. Nu există capacitatea necesară pentru a transmite numele de utilizatori și parolele la un serviciu de autentificare sau pentru a coordona procesele de criptare. Este evident că sistemele celulare 1G au fost proiectate să transporte vocea și nu datele.

Sistemele 1G acopereau, la un moment dat, cea mai mare parte a SUA. Astăzi, însă, acestea mai există doar în zonele care au o densitate scăzută a populației, acolo unde nu e realizabilă modernizarea infrastructurii pentru trecerea la noile sisteme digitale.

A doua generație de sisteme celulare

Nu cu multă vreme în urmă, au devenit disponibile sistemele celulare digitale, care permit ca atât canalele de voce cât și cele de control să utilizeze semnale digitale. Prima fază din realizarea sistemelor complet digitale este cunoscută sub numele de *a doua generație de sisteme celulare* (în limba engleză: second-generation cellular — acronim *2G cellular*) sau *sistem 2G*. Majoritatea operatorilor de telecomunicații din prezent posedă sisteme 2G, diverse îmbunătățiri apărând periodic.

Utilizarea semnalelor digitale pentru canalele de voce permite o modulare mai eficientă. Acest lucru oferă posibilitatea de a se realiza mai multe convorbiri telefonice și transmisii de date pe baza unui spectru de frecvențe redus. De fapt, sistemele 2G permit ca servicii mai avansate — cum ar fi autentificarea, mesajele text scurte și actualizarea telefonică a software-urilor — să poată fi accesate fără fir.

Versiuni îmbunătățite ale sistemelor 2G (numite uneori sisteme 2,5G) includ chiar modulări mai bune, care cresc vitezele de transmisie și eficiența folosirii spectrului de frecvențe. De exemplu, serviciul general pentru pachete radio (în limba engleză: General Packet Radio Service — acronim GPRS) oferă viteze înalte de transmisie prin intermediul rețelei sistemului global de comunicații mobile (GSM). Viteza de transmisie maximă prin GPRS este de 171,2 Kbps. Utilizarea GPRS necesită însă, un telefon mobil specializat. De asemenea, serviciul de viteze de transmisie îmbunătățite pentru evoluția globală (în limba engleză: Enhanced Data Rate for Global Evolution — EDGE) îmbunătățește performanțele GSM folosind o modulare PSK pe 8 niveluri, prin care fiecare simbol reprezintă 3 biți de date. Acest lucru duce la o viteză de transmisie maximă de 474 Kbps.

A treia generație de sisteme celulare

Mulți operatori de telecomunicații au început să ofere ceea ce este cunoscut sub numele de *a treia generație de sisteme celulare* (în limba engleză: third-generation cellular — acronim *3G cellular*) sau *sistem 3G*, care oferă un suport, chiar mai bun, pentru comunicațiile de date. Sistemele de telecomunicații mobile universale (în limba engleză: Universal Mobile Telecommunications Systems — UMTS) sunt capabile să asigure viteze de transmisie de 2 Mbps pentru implementările din interiorul clădirilor, până la 384 Kbps în zonele urbane și 144 Kbps în zonele rurale. Prin urmare, sistemele 3G pot accepta aplicații multimedia. A existat o dispută serioasă în industria sistemelor fără fir pe tema: sistemele 3G vor înlocui tehnica 802.11 (Wi-Fi) pentru LAN fără fir.

Având viteze de transmisie mai mari la utilizările în interiorul clădirilor, sistemele 3G sunt o alternativă la LAN-urile fără fir. Totuși, pentru rețelele 802.11 continuă să apară îmbunătățiri de performanțe care duc la depășirea semnificativă a performanțelor sistemelor 3G. De exemplu, standardul 802.11a specifică viteze de transmisie de 54 Mbps, care sunt mult mai mari decât cele asigurate de sistemele 3G. De asemenea, instalarea LAN-urilor fără fir este mai ieftină.

Totuși, LAN-urile fără fir nu sunt practice pentru asigurarea unei acoperiri pe arii întinse. Acest lucru ar necesita prea multă infrastructură. Sistemele 3G folosesc turnurile de celule existente și sistemele de distribuție aferente. Cheltuielile necesare

pentru trecerea de la sistemele 1G și 2G la sistemele 3G rămân încă ridicate, însă aceasta este cea mai convenabilă metodă pentru realizarea de rețele fără fir pe suprafețe întinse.

Astfel, sistemele 3G și sistemele LAN fără fir sunt complementare. Acest lucru a stimulat grupurile pentru standardizare și pe producători să găsească căi de a integra într-un sistem omogen sistemele 3G și LAN-urile fără fir. De fapt, sunt disponibile astăzi telefoane mobile și PDA-uri care implementează ambele tehnici. Având astfel de capacități, un utilizator se poate deplasa în afara razei de acțiune a unei LAN fără fir asociindu-se, în mod automat, cu un sistem celular. Problema este că standardele care definesc această formă de roaming nu sunt încă disponibile, ceea ce înseamnă că utilizatorul trebuie să aleagă cu atenție acei furnizori de servicii care acceptă telefonul mobil sau PDA-ul respectiv.

Aplicațiile SMS²

Unul dintre cele mai comune servicii oferite de WAN-urile fără fir este serviciul de mesaje scurte (SMS), care este un sistem de mesaje text capabil să transmită câteva sute de caractere o dată. SMS este o variantă fără fir a sistemului familiar de transmisie instantanee de mesaje care este oferit de mulți furnizori de servicii Internet (ISP). În continuare sunt enumerate aplicații suplimentare ale SMS, utilizabile pe baza WAN-urilor fără fir:

- **Livrări de conținut** — SMS asigură livrarea eficientă a actualizărilor pentru dispozitivele de utilizatori. De exemplu, un utilizator poate descărca, prin SMS, noi tonuri de apel și fundaluri fanteziste pentru telefonul său. În plus, SMS face posibilă interogarea unei baze de date de către utilizatori precum și alimentarea cu știri a utilizatorilor. De exemplu, puteți fi ținut la curent cu ultimele știri prin primirea de informații curente prin SMS.
- **Alerte** — Majoritatea operatorilor oferă o varietate de alerte, cum ar fi alerta pentru mesaje vocale aflate în așteptare, anunțarea scorurilor sportive, informații despre prețurile curente ale acțiunilor la bursă și alte memento-uri. Acest lucru vă permite să primiți informații atunci când se întâmplă un lucru pe care dumneavoastră îl considerați important.
- **Interacțiuni** — Unele show-uri de televiziune permit interactivitatea între telespectatori și gazde prin intermediul SMS. Acest lucru asigură participarea telespectatorilor la emisiune, ceea ce duce la o creștere spectaculoasă a audienței.

² În limba engleză: Short Message Service (n.tr.).

- **Integrarea în aplicații** — Există posibilitatea ca producătorii să integreze SMS în multe aplicații de corporație. De exemplu, o companie poate avea un sistem de management al vânzărilor care să permită reprezentanților de vânzări să urmărească clienții și produsele. O companie poate, în mod obișnuit, să completeze cu ușurință aceste aplicații cu SMS. De exemplu, adăugarea unui mecanism de alertare poate fi benefică. Reprezentanții de vânzări vor putea fi anunțați atunci când un produs nu mai este pe stoc. Multe site-uri Web folosesc limbajul de marcare fără fir (în limba engleză: Wireless Markup Language — acronim WML) pentru a transforma paginile Web obișnuite într-un format care este mai ușor de citit pe un dispozitiv de mici dimensiuni, cum ar fi un PDA sau un telefon celular. WML reduce și grafica paginii Web pentru a compensa viteza de transmitere a datelor care este mai scăzută la tehnicile WAN fără fir.

Notă



Pentru mai multe informații despre aplicații cu transmitere instantanee de mesaje vizitați Planeta mesajelor transmise instantaneu (Instant Messaging Planet) la <http://www.instantmessagingplanet.com>.

WAN-uri fără fir bazate pe spațiu

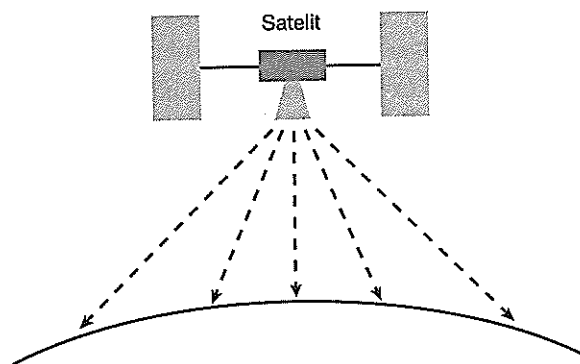
Pe lângă sistemele celulare cu baza la sol, utilizarea sistemelor bazate pe spațiu furnizează mijloacele pentru conectarea utilizatorilor pe suprafețe vaste.

Satețiți

Utilizarea sateliților pentru transmisiile de televiziune și pentru alte comunicații se realizează de câteva decenii. Însă, până de curând, sateliții nu au fost folosiți pentru conectarea la Internet a utilizatorilor (vezi figura 7.7). Vitezele de transmisie sunt apreciable, ajungând până la 1,5 Mbps pe fluxul descendent.

Unele sisteme bazate pe satelit asigură două căi de schimb de date, permițând unui utilizator să trimită date la satelit și să primească date de la acesta. De exemplu, un dispozitiv mobil al unui utilizator poate transmite o solicitare pentru o pagină Web la satelit, iar acesta o retransmite înapoi la sol, stației terestre adecvate. Stația terestră trimite apoi pagina Web la satelit, iar acesta o retransmite utilizatorului. Însă, alte sisteme bazate pe satelit asigură doar legătura dinspre satelit către sol. Dispozitivul utilizatorului trebuie să solicite pagina Web printr-o altă rețea, cum ar fi printr-o legătură telefonică, iar satelitul va transmite pagina la utilizator.

Figura 7.7. Sistemele bazate pe sateliți extind în mod spectaculos ariile de acoperire ale WAN-urilor fără fir



Prin încorporarea de repetoare radio active în sateliții artificiali de pe orbita Pământului este posibil să se realizeze transmisii radio și comunicații punct-la-punct pe zone mari de pe suprafața Pământului. Capacitatea de transmisie a unui repetoare de satelit este remarcabilă și, prin selectarea unor moduri de emisie adecvate pentru antena satelitului, se poate realiza acoperirea unor suprafețe terestre bine definite.

Sateliții sunt poziționați în diferite puncte de pe o orbită geostaționară, în funcție de cerințele misiunii îndeplinite de sistem. Pentru a obține acoperire globală sunt necesari minim trei sateliți. Însă, pentru a obține nivele de constanță acceptabile pentru semnalele RF sunt desfășurați patru sateliți. Acest lucru asigură și o oarecare libertate de poziționare a acestora.

Pentru comunicațiile prin satelit sunt folosite frecvențe favorabile transmisiei ceea ce duce la: utilizarea eficientă a energiei, distorsiuni de propagare minime și o susceptibilitate minimă la zgomot și la interferențe. Din nefericire, sistemele terestre tind să utilizeze și ele aceste frecvențe. Spațiul este un domeniu internațional, iar Uniunea Internațională pentru Telecomunicații (în limba engleză: International Telecommunications Union — ITU) este cea care controlează frecvențele pentru sateliți.

Banda de frecvențe dintre 450 MHz și 20 GHz este cea mai potrivită pentru legături radio Pământ-spațiu-Pământ. Nu este practic să se stabilească legături cu un terminal terestru aflat într-o regiune climatică cu ploi abundente la frecvențe mai mari de 20 GHz, dacă se așteaptă ca acestea să fie disponibile în majoritatea timpului.

Pentru toate benzile de operare, spectrul de frecvențe cel mai scăzut este utilizat pentru legătura radio descendentă (de la satelit la sol), deoarece acesta are cele mai severe limitări de putere. Frecvențele mai scăzute sunt mai puțin sensibile la atenuare

în spațiul liber, prin comparație cu frecvențele mai înalte, utilizate pentru legăturile radio ascendente. Pierderile sunt mai ușor de compensat pe legăturile ascendente care dispun de puterea de transmisie mai mare a stațiilor terestre.

Satelitul se comportă ca un repetoare de semnale. Semnalele primite prin legătura ascendentă sunt redifuzate spre Pământ prin legătura descendentă. Dispozitivul care se ocupă de această acțiune este numit transponder. Transponderul unui satelit este analog cu repetoarul din legăturile de comunicații terestre; acesta trebuie să recepționeze, să amplifice și să retransmită semnalele venite de la terminalele terestre. Transponderul unui satelit este capabil să acționeze ca un repetoare pentru una sau mai multe legături de comunicații RF.

Sateliții de joasă altitudine, care au orbite circulare, polare sau înclinate, au perioade orbitale mai scurte de 24 de ore. În consecință, aceștia par a se mișca atunci când sunt văzuți de pe suprafața Pământului. Aceste tipuri de orbite sunt utile pentru scopuri legate de supraveghere și pot fi utilizate pentru asigurarea comunicațiilor la latitudini extreme, nordice sau sudice.

Unul dintre tipurile de orbită de interes pentru comunicațiile publice de date este orbita geostaționară. Un satelit aflat pe o astfel de orbită are o perioadă de revoluție de 24 de ore la o altitudine de aproximativ 36 000 de kilometri și rămâne deasupra unei locații fixe de pe ecuator. Prin urmare, pentru un observator de pe Pământ, satelitul pare a nu se mișca.

În realitate, satelitul nu rămâne, cu adevărat, fix. Chiar dacă orbita ar fi perfect circulară și la altitudinea exactă necesară, fenomene naturale (datorate câmpurilor gravitaționale slabe ale Lunii și ale altor planete și presiunii radiației solare) produc deplasări ale orbitei. Aceste deplasări minore și lente sunt corectate periodic de mici rachete aflate la bordul sateliților, care sunt activate de la stațiile terestre.

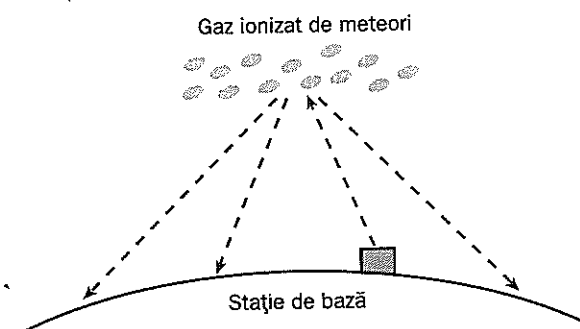
Datorită lungimii mari a căii de propagare (aproximativ 36 000 de kilometri de la terminalul terestru până la un satelit aflat pe o orbită geostaționară) se produce o întârziere a transmisiei de aproximativ 100 ms (milisecunde) între terminalul terestru și satelit. Acest lucru conduce la o întârziere aproximativă de 200 ms pentru traseul Pământ-satelit-Pământ. Acest lucru face ca, pentru un astfel de sistem, utilizarea protocoalelor (cum ar fi 802.11) să fie inefficientă, deoarece acestea solicită un răspuns după fiecare pachet de informații transmis, înainte de transmiterea următorului pachet. De fapt, majoritatea protocoalelor de rețea nu funcționează eficient prin legăturile prin satelit deoarece protocoalele așteaptă confirmări rapide de la destinație.

Comunicații bazate pe arderea meteorilor în atmosfera terestră

Miliarde de meteori microscopici pătrund în atmosfera terestră. De fapt, meteorii cad adesea pe timpul unei zile deasupra tuturor zonelor de pe glob. Atunci când acești meteori pătrund în atmosfera terestră, la mari altitudini, se transformă într-un gaz ionizat. Acest gaz este văzut ca o stea căzătoare, care este un meteor mare și rar, prin comparație cu majoritatea celorlalți.

Cunoscute sub numele de sistemul de satelit al omului sărac, comunicațiile bazate pe arderea meteorilor (vezi figura 7.8) se realizează prin reflectarea semnalelor RF de către gazul ionizat de meteori. Acest lucru permite realizarea unor legături de transmisii de date fără fir, la mare distanță (2 500 de kilometri) fără cheltuielile necesare pentru lansarea și întreținerea unui satelit.

Figura 7.8. Sistemele bazate pe arderea meteorilor folosesc gazul ionizat de meteori pentru a reflecta semnalele înapoi pe Pământ



Comunicațiile bazate pe arderea meteorilor direcționează, spre gazul ionizat, unde radio cu frecvențe de 40-50 MHz, modulate cu datele semnalului. Apoi semnalul radio este reflectat de gaz, fiind direcționat înapoi către Pământ. Disponibilitatea transmisiilor bazate pe gazul ionizat este bună, dar acesta este prezent adesea doar atât cât să asigure viteze de transmisie de la 300 bps la 2 400 bps. Acestea sunt valori foarte mici, chiar prin comparație cu modemurile telefonice.

Totuși, costurile instalării de echipamente bazate pe arderea meteorilor sunt atât de scăzute prin comparație cu cele ale sistemelor bazate pe sateliți, încât aplicațiile care necesită performanțe scăzute, cum ar fi telemetria, sunt realizabile. De exemplu, sistemele bazate pe arderea meteorilor funcționează corespunzător pentru transmiterea nivelelor zăpezii din munții aflați la mare distanță, către centrele de monitorizare.

Tehnici WAN fără fir

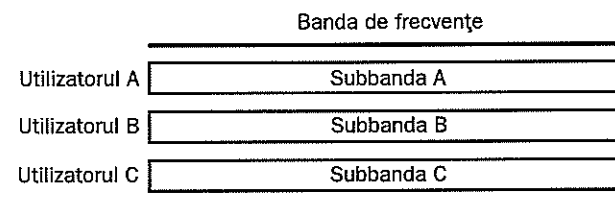
WAN-urile fără fir utilizează tehnici concentrate pe modularea de voce și de date. Așa cum am discutat în capitolul 2, intitulat *Arhitectura sistemului fără fir: cum funcționează rețelele fără fir*, semnalele digitale, care reprezintă informațiile în interiorul unui calculator, sunt convertite prin modulare în semnale RF sau semnale de lumină. WAN-urile fără fir utilizează exclusiv semnale RF destinate să servească multor utilizatori. Fiecare utilizator are un canal dedicat, spre deosebire de LAN-urile fără fir în care utilizatorii partajează un singur canal. Acest lucru reduce semnificativ interferențele produse între dispozitivele pentru utilizatori de WAN-uri fără fir și stațiile de bază.

Să aruncăm o privire mai atentă asupra diverselor tehnici de modulare.

Accesul multiplu prin divizarea spectrului de frecvențe

Accesul multiplu prin divizarea spectrului de frecvențe (în limba engleză: *Frequency Division Multiple Access* — acronim *FDMA*) împarte o bandă largă de frecvențe în sub-benzi mai mici, fiecare utilizator folosind sub-banda care i-a fost atribuită pentru transmiterea de voce și de date. Toți utilizatorii își transmit semnalele simultan. Figura 7.9 ilustrează acest concept. Sistemele celulare tradiționale 1G utilizează FDMA pentru transmisia de date.

Figura 7.9. FDMA permite transmisii simultane deoarece utilizatorii nu operează în aceeași porțiune a spectrului de frecvențe



Comunica

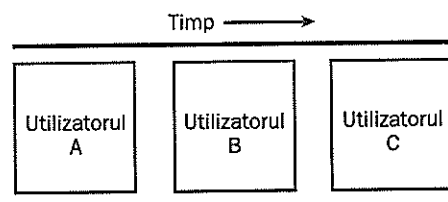
Miliard
cad ades
acești n
gaz ie
prin
ile

165

vea timpului de transmisie

Accesul multiplu prin divizarea timpului (în
access — acronim *TDMA*) separă utilizatorii
să transmită la un moment de timp dat. Fiecare
să transmită în care poate transmite. Unii dintre opera-
ai vechi utilizează TDMA pentru a oferi conexiuni de voce
ul WAN-urilor fără fir. De exemplu, circuitele T1 folosesc
combina conexiuni de utilizatori separate prin același circuit.

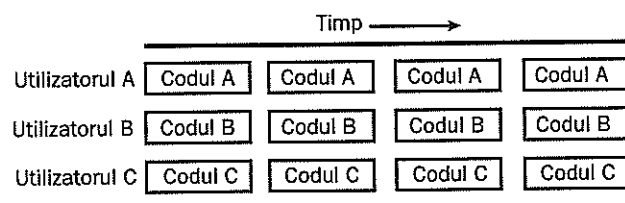
TDMA face astfel ca utilizatorii să transmită numai pe perioada
ferestrei de timp care le-a fost atribuită



Accesul multiplu cu divizare prin cod

Similar cu FDMA, *accesul multiplu cu divizare prin cod* (în limba engleză: *code division multiple access* — acronim *CDMA*), permite realizarea de transmisii simultane (vezi figura 7.11). Diferența constă, însă, în aceea că utilizatorii CDMA pot ocupa întreaga bandă de frecvențe simultan. Utilizatorii nu au de-a face cu interferențele pentru că fiecare dintre ei își modulează semnalul folosind un cod diferit. Un avantaj al CDMA este acela că dispozitivele utilizatorilor se pot conecta la mai multe stații de bază datorită codurilor diferite. Acest lucru duce la creșterea performanțelor și la fiabilitate. Sistemele celulare folosesc, în mod predominant, rețelele fără fir CDMA.

Figura 7.11. CDMA atribuie fiecărui utilizator un cod, ceea ce face posibil ca utilizatorii să transmită simultan, fără apariția interferențelor



Accesul multiplu prin divizare spațială

Accesul multiplu prin divizare spațială (în limba engleză: *spatial division multiple access* — acronim *SDMA*) asigură accesul mai multor utilizatori prin focalizarea unui fascicul pentru fiecare utilizator. Acest tip de acces este comun pentru sistemele bazate pe sateliți. Unele sisteme SDMA sunt adaptive, fasciculul radio urmărind mișcările utilizatorului. În cazul altor sisteme trebuie ca dispozitivul utilizatorului să se asocieze cu următorul fascicul, pe măsură ce utilizatorul se deplasează.

Notă



Unele dispozitive WAN fără fir, cum ar fi telefoanele mobile, au mai multe moduri sau benzi și acceptă mai multe tehnici de transmisie. De exemplu, un singur telefon mobil poate accepta atât TDMA, cât și CDMA. Telefonul comută, în mod automat, de la o tehnică la alta, în funcție de rețeaua care este disponibilă.

Rezumatul capitolului

WAN-urile fără fir sunt formate din turnuri de celulă, antene parabolice, sateliți și infrastructură de comunicații. Majoritatea aplicațiilor WAN-urilor fără fir fac uz de conexiuni exterioare clădirilor, însă unele amenajări interioare, cum ar fi aeroporturile și centrele de conferințe, instalează WAN-uri fără fir atunci când există un număr mare de abonați. Infrastructura WAN-urilor fără fir este scumpă prin comparație cu cea a celorlalte tipuri de rețele fără fir, însă WAN-urile fără fir sunt cele mai potrivite pentru a acoperi zone de dimensiunile unor țări sau continente. Sistemele celulare și cele bazate pe sateliți sunt cele mai comune forme de WAN-uri fără fir capabile să realizeze performanțe moderate. Comunicațiile bazate pe reflectarea undelor radio de către gazul ionizat prin arderea meteorilor sunt mai ieftine, însă oferă numai performanțe scăzute.



Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. Care sunt cele mai comune tipuri de dispozitive pentru utilizatorii WAN-urilor fără fir?
2. De ce operatorii de WAN-uri fără fir taxează întotdeauna serviciile oferite?
3. De ce trebuie să fiți atent atunci când alegeți o placă NIC radio WAN fără fir pentru dispozitivul dumneavoastră de utilizator?
4. Care este unul dintre avantajele utilizării unui sistem bazat pe satelit?
5. Ce generație de sisteme celulare oferă viteze de transmisie a datelor de până la 2 Mbps?
6. Care este cel mai comun tip de sistem WAN fără fir?
7. Care dintre următoarele două tipuri de sisteme celulare oferă viteze de transmisie a datelor mai mari: GPRS sau UMTS?
8. Care este principala problemă legată de comunicațiile bazate pe reflexia undelor radio pe stratul de gaze ionizate produse de arderea meteorilor?
9. Adevărat sau fals: FDMA solicită utilizatorilor să își aștepte rândul pentru a-și transmite semnalele.
10. Cum evită CDMA posibilitatea ca utilizatorii să-și producă, unul altuia, interferențe?

Ce veți învăța

După citirea acestui capitol, veți putea:

- ✓ să înțelegeți chestiunile legate de securitatea rețelelor fără fir;
- ✓ să descrieți metodele care pot contracara problemele de securitate întâmpinate;
- ✓ să înțelegeți bazele tehnicilor de criptare și autentificare și standardele legate de acestea.



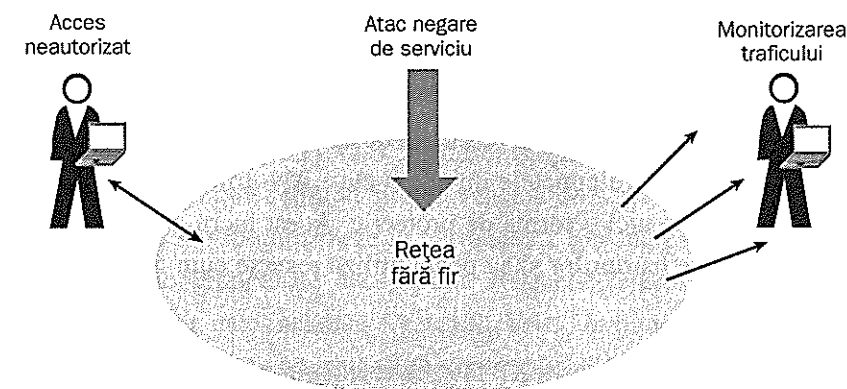
Securitatea rețelelor fără fir: protejarea resurselor de informații

Protecția/securitatea datelor este importantă pentru rețelele fără fir, în primul rând deoarece semnalele comunicațiilor se află la dispoziția oricui în timpul propagării lor prin aer. Companiile și persoanele care utilizează rețele fără fir trebuie să fie conștiente de problemele potențiale și trebuie să știe care sunt contramăsurile aplicabile. Acest capitol discută amenințările la adresa securității și căile de întărire a securității rețelelor fără fir prin folosirea *criptării* și a *autentificării*.

Amenințările la adresa securității rețelelor

Așa cum se arată în figura 8.1, există câteva tipuri de amenințări la adresa securității rețelelor fără fir. De exemplu, *hackerii* pot fura informații dintr-o companie, pot obține accesul neautorizat la aplicații și pot chiar să întrerupă funcționarea unei rețele.

Figura 8.1. Amenințările la adresa securității unei rețele fără fir includ: monitorizarea pasivă, accesul neautorizat și atac negare de serviciu (DoS)



Monitorizarea traficului

Un hacker experimentat, sau chiar un *curios* (în limba engleză: *snooper*), poate să monitorizeze cu ușurință pachetele de date transmise prin rețelele fără fir neprotejate, folosind instrumente cum ar fi AirMagnet și AiroPeek, care dezvăluie în întregime conținuturile pachetelor de date transmise. De exemplu, curioșii, aflați la câteva zeci de metri de o clădire care conține o LAN fără fir, pot monitoriza toate transferurile de date realizate prin porțiunea fără fir a rețelei. Desigur, problema constă în faptul că oricine poate identifica numele de utilizatori, parolele, numerele cărților de credit și așa mai departe. De fapt, purtătorii acestui război își și expun „descoperirile” pe un site Web, doar pentru a se distra.

Soluționarea acestei probleme se poate face, la un nivel minimal, prin criptarea datelor transmise între dispozitivul fără fir client și stația de bază. Criptarea modifică biții de date, folosind o cheie secretă. Deoarece cheia este secretă, un hacker nu va putea să descifreze datele. În concluzie, utilizarea unui mecanism de criptare eficace păstrează confidențialitatea datelor.

Accesul neautorizat

Asemănător cu cazul monitorizării unei aplicații fără fir, cineva, aflat în afara sediului, poate să acceseze, fără efort, o rețea fără fir de corporație dacă nu sunt luate măsurile preventive cuvenite. Persoana respectivă poate, de exemplu, să stea într-o mașină parcată lângă sediu și să se asocieze cu una dintre stațiile de bază fără fir localizate în interiorul clădirii. În absența unor măsuri de securitate adecvate, această persoană poate accesa servere și aplicații care țin de rețeaua de corporație. Aceasta este ca și cum a-ți lăsa un străin să intre în locuința sau în sediul dumneavoastră.

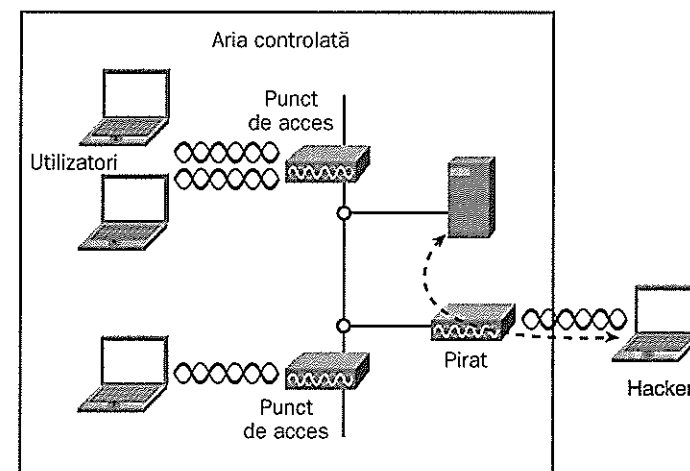
Din nefericire, multe companii își instalează rețelele fără fir folosind configurațiile prestabilite ale stațiilor de bază, care nu asigură securitatea, făcând astfel posibil ca oricine să poată accesa serverele lor de aplicații. De fapt, dacă veți verifica, veți constata că 30% dintre punctele de acces ale LAN-urilor fără fir dintr-un oraș obișnuit nu au instalate nici o formă de protecție. Acest lucru permite ca oricine să poată accesa drivelele hardurilor și să poată utiliza resurse cum ar fi conexiunile cu Internetul.

Sistemul de operare Windows XP face ca realizarea unei interfețe cu o rețea fără fir să fie facilă, mai ales dacă aceasta este o rețea LAN fără fir publică. Atunci când

un laptop se asociază la o rețea LAN fără fir, utilizatorul poate naviga prin oricare alt laptop asociat la aceeași rețea LAN fără fir. Fără protecția unui *parafoc*¹ personal, cineva poate accesa informațiile de pe hard discul dumneavoastră. Acest lucru constituie un risc major de securitate.

Chiar dacă implementați toate controalele de securitate la punctele de acces, posibilitatea conectării prin intermediul unui *punct de acces pirat* (în limba engleză: *rogue access point*) constituie o amenințare importantă la adresa securității rețelei (vezi figura 8.2). Un punct de acces pirat este un punct de acces neautorizat, plasat în rețea. Un angajat poate cumpăra un punct de acces și îl poate instala în biroul său fără să cunoască implicațiile pe care acest fapt le are asupra securității rețelei. De asemenea, un hacker poate planta un punct de acces pirat în interiorul sediului firmei, cu intenția de a conecta un punct de acces neprotejat la rețeaua de corporație.

Figura 8.2. Un punct de acces pirat oferă un port deschis pe care hackerii îl pot exploata



Un punct de acces pirat poate fi exploatat, deoarece este probabil că nu va avea nici o criptare activată, ceea ce oferă o ușă deschisă pentru cineva care poate accesa astfel, cu ușurință, din afara sediului firmei, rețeaua de corporație. Din acest motiv, o companie trebuie să-și monitorizeze în permanență rețeaua pentru a depista eventuala prezență a unor puncte de acces pirat. Rețineți că acest lucru constituie o problemă chiar dacă nu este instalată o rețea fără fir. Un punct de acces pirat poate fi conectat de către cineva și la o rețea Ethernet realizată în totalitate prin fire.

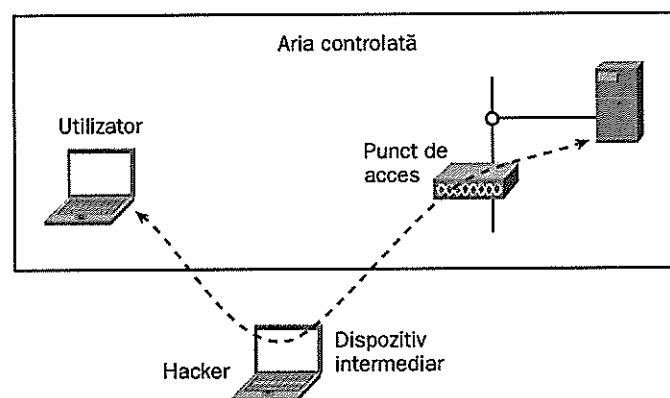
¹ În limba engleză, firewall (n.tr.).

Pentru a contracara accesul neautorizat, rețelele fără fir trebuie să implementeze autentificarea reciprocă între dispozitivele client și punctele de acces. Autentificarea este acțiunea de dovedire a identității unei persoane sau a unui dispozitiv. Rețelele fără fir trebuie să implementeze metode prin care dispozitivele clienți să-și dovedească identitatea în raport cu punctele de acces și viceversa. Acest lucru garantează validitatea utilizatorilor și dovedește că aceștia se conectează la puncte de acces legitime. În plus, punctele de acces trebuie să se autentifice în raport cu comutatoarele pentru a respinge tentativa de conectare a unui punct de acces pirat.

Atacuri de tipul omul-la-mijloc

Utilizarea tehnicilor de criptare și autentificare îmbunătățește protecția rețelelor fără fir; însă, hackerii inteligenți pot totuși găsi puncte vulnerabile datorită modului în care funcționează protocoalele de rețea. Un punct slab bine definit este exploatat de atacul omul-la-mijloc, care se produce atunci când un hacker plasează un dispozitiv fictiv între utilizatori și rețeaua fără fir (vezi figura 8.3). De exemplu, un atac comun de tipul omul-la-mijloc se poate folosi de protocolul de conversie a adreselor (ARP), care este un protocol uzual utilizat de toate rețelele TCP/IP. Un hacker dotat cu un instrument adecvat se poate folosi de ARP pentru a prelua controlul rețelei fără fir.

Figura 8.3. Dispozitivele intermediare permit atacuri de tipul omul-la-mijloc



ARP este o funcție crucială utilizată de o NIC cu, sau fără, fir transmițătoare pentru a afla care este adresa fizică a plăcii de rețea destinare. Adresa fizică a unei plăci este adresa de control a accesului la mediu (MAC), care este înglobată în placa

de rețea de către producător și care este unică (nu există o altă placă sau o altă componentă de rețea cu aceeași adresă). Adresa MAC este analoagă cu adresa locuinței dumneavoastră. Așa cum cineva trebuie să cunoască această adresă pentru a putea să vă trimită o scrisoare, o NIC transmițătoare trebuie să cunoască adresa MAC de destinație. Placa de rețea înțelege doar adresa MAC, iar atunci când răspunde face uz de aceasta.

Software-ul de aplicație care trebuie să transmită datele cunoaște adresa IP de destinație, însă placa de rețea care transmite trebuie să folosească ARP pentru a afla adresa fizică care corespunde adresei IP. Placa obține adresa difuzând un pachet solicitare ARP care anunță adresa IP a plăcii de rețea de destinație. Toate stațiile vor auzi această solicitare, iar stația care are respectiva adresa IP va întoarce un pachet răspuns ARP, care conține adresa sa MAC și adresa sa IP.

Apoi, stația transmițătoare va include această adresă MAC, ca adresă de destinație a cadrului care va fi transmis. De asemenea, stația transmițătoare va memora adresa IP și adresa MAC corespunzătoare acestuia, într-un tabel, pentru o anumită perioadă de timp (sau până când stația va primi un alt răspuns ARP de la stația care are respectiva adresa IP).

O problemă legată de ARP este aceea că introduce un risc la adresa securității rețelei ca rezultat al înșelării protocolului de conversie a adreselor (ARP) de către cineva. De exemplu, un hacker poate înșela o stație prin transmiterea unui răspuns ARP fictiv, de la un dispozitiv de rețea pirat, răspuns care include adresa IP a unui dispozitiv de rețea legitim și adresa MAC a dispozitivului pirat. Acest lucru face ca toate stațiile legitime din rețea să-și actualizeze, în mod automat, tabelele lor ARP cu această falsă corespondență între adrese.

Bineînțeles că aceste stații vor transmite apoi pachetele următoare la dispozitivul pirat, în loc să le transmită la routerul sau punctul de acces legitim. Acesta este un atac clasic de tipul omul-la-mijloc, atac care permite unui hacker să manipuleze sesiunile unui utilizator. Prin urmare, hackerul poate afla parole, poate obține date secrete și poate chiar să se conecteze la serverele de corporație ca și cum ar fi un utilizator legitim.

Pentru a dejuca atacurile de tipul omul-la-mijloc realizate prin înșelarea ARP, producătorii, cum ar fi OptimumPath, implementează ARP sigur (în limba engleză: secure ARP — acronim SARP). Această versiune îmbunătățită a ARP asigură un

tunel sigur special între fiecare client și punctul de acces sau routerul fără fir, ignorând orice răspuns ARP care nu este asociat cu unul din clienții de la celălalt capăt al tunelului. În consecință, doar răspunsurile ARP legitime vor constitui baza pentru actualizarea tabelor ARP. Stațiile care implementează SARP nu pot fi înșelate.

Însă, utilizarea SARP presupune instalarea unui software special la fiecare client. Prin urmare, SARP nu este o soluție practică pentru punctele fierbinți publice. Totuși, companiile pot instala SARP pe dispozitivele client, fiind astfel mult mai ferite de atacuri de tipul omul-la-mijloc.

Negare de serviciu

Un atac negare de serviciu (în limba engleză: Denial of Service — acronim DoS) este un atac care poate afecta funcționarea unei rețele fără fir sau o poate scoate din funcțiune. Posibilitatea producerii unui astfel de atac trebuie luată în considerație de oricine instalează o rețea fără fir. Trebuie să luați în calcul ce s-ar putea întâmpla dacă rețeaua fără fir ar deveni indisponibilă pentru o perioadă de timp nedefinită.

Gravitatea unui atac DoS depinde de impactul pe care îl poate avea inactivarea rețelei fără fir. De exemplu, un hacker poate scoate din funcțiune un LAN fără fir din locuința cuiva, însă acest fapt va produce, probabil, neplăceri numai proprietarului locuinței. Însă, un atac DoS care scoate din funcțiune un sistem fără fir de verificare a inventarului poate produce pierderi financiare majore.

Una dintre formele de atac DoS este metoda forței brute. De exemplu, o revărsare a unui număr foarte mare de pachete de date, care folosesc toate resursele rețelei și o forțează pe aceasta să se oprească din funcționare, este un atac DoS de tip forță brută. Există, în Internet, instrumente care oferă unui hacker posibilitatea de a produce o revărsare excesivă de pachete de date asupra unei rețele fără fir. Un hacker poate realiza un atac DoS tip forță brută, bazat pe revărsarea de pachete, prin transmiterea de pachete inutile la server de către alte calculatoare din rețea. Acest lucru supraîncarcă semnificativ rețeaua și ocupă lărgimea de bandă care ar putea fi folosită de către utilizatorii legitimi.

O altă cale de oprire a funcționării majorității rețelelor fără fir, mai ales a celor care utilizează *accesul cu sesizarea purtătoarei*, este folosirea unui semnal radio puternic care să domine undele aeriene și care face ca punctele de acces și plăcile radio să fie inutile. Protocoalele, cum ar fi 802.11, sunt foarte „politicoase” și cedează accesul la mediu semnalului de atac DoS pentru oricât de mult timp dorește atacatorul.

Totuși, utilizarea unui semnal radio puternic pentru a întrerupe funcționarea rețelei este un atac destul de riscant pentru un hacker. Deoarece pentru executarea unui astfel de atac este necesar un emițător puternic, aflat la mică distanță de rețea, proprietarii acestuia pot să-l descopere pe hacker cu ajutorul instrumentelor de localizare puse la dispoziție de analizoarele de rețea. O dată ce sursa de bruiaj este găsită, autoritățile o pot opri și este posibil să-i descopere și pe vinovați.

Uneori, o negare de serviciu poate să apară într-o rețea fără fir în mod neintenționat. De exemplu, rețelele 802.11b funcționează într-un spectru radio aglomerat. Alte dispozitive, cum ar fi telefoanele fără fir, cuptoarele cu microunde și dispozitivele Bluetooth pot produce reduceri semnificative ale performențelor rețelelor 802.11b. Astfel de interferențe pot opri funcționarea unei rețele fără fir.

În plus, unele mecanisme de securitate constau în țintele predilecte ale atacurilor DoS. De exemplu, accesul protejat Wi-Fi (WPA) este vulnerabil la tipul de atac DoS. WPA folosește algoritmi matematici pentru a autentifica utilizatorii unei rețele. Dacă un utilizator se conectează și transmite, într-un interval de o secundă, două pachete de date neautorizate, WPA va presupune că acesta este un atac și va opri funcționarea rețelei.

Singura cale complet eficace de a contracara atacurile DoS este să izolați calculatorul dumneavoastră într-o încăpere foarte bine protejată și să-l deconectați de la toate rețelele, inclusiv de la Internet. Acest lucru peresupune, binențeles, că nu veți utiliza o rețea fără fir. Guvernul SUA folosește această metodă pentru a-și proteja datele cele mai importante, însă această soluție nu este practică pentru orice aplicație de întreprindere sau de locuință, cazuri în care instalarea de rețea fără fir aduce beneficii.

Cea mai importantă metodă de apărare față de atacurile DoS este menținerea unor practici solide de securitate. Acțiuni cum ar fi implementarea și actualizarea parafo-curilor, întreținerea unor software-uri antivirus actualizate, instalarea unor măsuri de securitate la zi, utilizarea unui sistem solid de parole și întreruperea funcționării unor dispozitive de rețea când nu este nevoie de acestea trebuie să fie practici de rutină pentru toate firmele și pentru deținătorii de rețea la domiciliu.

Puteți proteja o LAN fără fir împotriva atacurilor DoS făcând în așa fel încât clădirea să reziste, pe cât posibil, la pătrunderea de semnale radio din exterior. Iată câteva măsuri care vă pot ajuta să realizați acest lucru:

- Dacă pereții interiori posedă stâlpi metalici, asigurați-vă că aceștia sunt legați la pământ.

- Montați ferestre izolate termic pe bază de film metalic.
- Folosiți acoperiri metalice pentru ferestre, în locul jaluzelelor sau perdelelor.
- Efectuați teste pentru a determina cât de departe ajung efectiv semnalele radio care scapă din clădire. Ajustați puterea de emisie în mod corespunzător până când scăpările sunt eliminate sau reduse până la nivelul care să facă ușoară localizarea unui hacker.
- Îndreptați antenele direcționale ale punctelor de acces către interiorul clădirii.

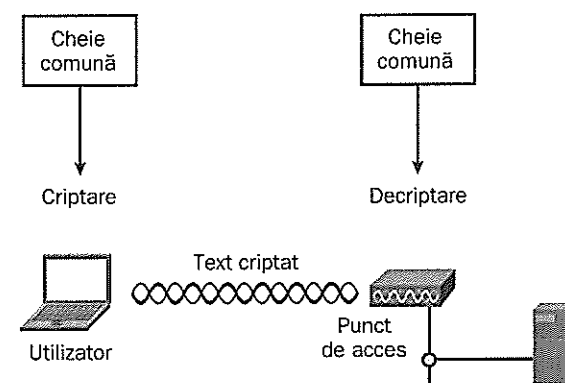
Deoarece nu există o modalitate de a contracara complet toate tipurile de atacuri DoS, aveți în vedere un plan de rezervă pentru cazul în care un atac DoS va produce distrugerii importante. De exemplu, să aveți o procedură de trecere la o procesare pe loturi sau la metode bazate pe hârtie dacă aplicația este supusă unui atac DoS grav. Cu siguranță că nu doriți ca slăbiciunile potențiale ale rețelei fără fir să vă doboare compania!

Criptarea

Criptarea modifică biții fiecărui pachet de date pentru a se evita situația în care anumite date, cum ar fi numerele cărților de credit, ar putea fi decodate de către curioși. Înainte de criptare datele sunt numite text simplu (în limba engleză: plain-text), text care este simplu de decodat prin utilizarea instrumentelor de monitorizare a rețelei. Criptarea convertește textul simplu în text criptat, care poate fi decodat doar de către cineva care utilizează o cheie secretă potrivită.

Multe metode de criptare, cum ar fi și *Wired Equivalent Privacy (WEP)* care este definită de standardul 802.11, sunt simetrice — ceea ce înseamnă că aceeași cheie prin care se realizează criptarea este folosită și pentru decriptare. Figura 8.4 ilustrează acest proces.

Figura 8.4. Criptarea simetrică utilizează o cheie comună



De exemplu, placa de rețea radio folosește cheia xyz pentru a cripta un pachet de date, iar punctul de acces utilizează tot cheia xyz pentru a realiza decriptarea. Acest lucru necesită să existe încredere reciprocă între stația emițătoare și cea receptoare, cum se întâmplă în cazul aplicației unei rețele fără fir private, cum este o LAN fără fir de întreprindere. Însă, nu este practic să se utilizeze chei simetrice pentru aplicațiile publice, pentru că oricine, inclusiv un hacker, poate afla cheia.

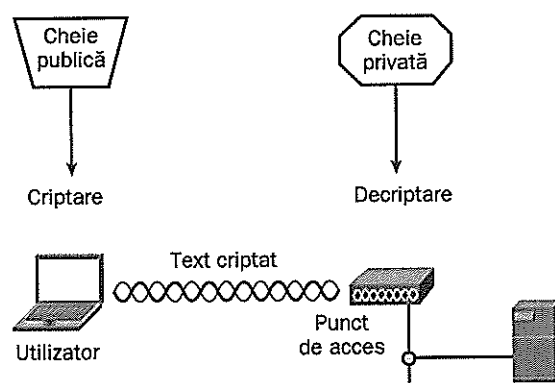
Pentru ca metoda criptării simetrice să fie eficace, funcția trebuie să micșoreze numărul de re folosiri ale unei chei prin dese schimbări ale cheii, dacă este posibil la transmisia fiecărui cadru. Acest lucru face ca timpul avut la dispoziție de un hacker pentru a pătrunde în rețea să fie scurt și astfel compromiterea securității rețelei va fi dificilă — dacă nu imposibilă. Prin urmare, mecanismele de criptare simetrică trebuie să dispună de metode eficiente de distribuire a cheii.

Criptarea cu cheie publică folosește chei asimetrice, dintre care una este privată, iar cealaltă este publică. Așa cum arată și numele, cheia privată este secretă, însă oricine poate afla cheia publică. Acest lucru permite utilizarea de mecanisme de criptare și de autentificare mai eficiente, deoarece simplifică procesul de distribuție a cheilor.

O cerință importantă a criptării cu cheie publică este aceea că un set format dintr-o cheie publică și una privată trebuie să se potrivească din punct de vedere criptografic. De exemplu, stația emițătoare poate cripta datele folosind cheia publică, iar receptorul folosește cheia privată pentru decriptare. Situația inversă este și ea adevărată. Stația emițătoare poate cripta datele folosind cheia privată, iar stația de recepție decriptează datele utilizând cheia publică.

Dacă scopul este să se cripteze datele, stația emițătoare va folosi o cheie publică pentru a cripta datele înainte de a le transmite; acest lucru este prezentat în figura 8.5. Stația receptoare folosește cheia privată corespunzătoare pentru a decripta datele, după ce le recepționează. Fiecare stație își păstrează secretă cheia privată pentru a evita descifrarea informației criptate. În consecință, procesul permite oricărei stații să folosească o cheie cunoscută public pentru a transmite date criptate oricărei alte stații.

Figura 8.5. Criptarea cu cheie publică permite tuturor transmițătorilor de date criptate să utilizeze o cheie disponibilă public



Criptarea cu cheie publică funcționează eficient pentru criptarea de date deoarece cheia publică poate fi disponibilă pentru oricine dorește să transmită date criptate unei anumite stații. O stație care generează o cheie privată nouă poate distribui cheia publică corespunzătoare acesteia oricui, prin intermediul rețelei, fără să fie preocupată că va compromite criptarea. Cheia publică poate fi afișată pe un site Web sau poate fi transmisă necriptată prin intermediul rețelei.

Criptarea WEP

WEP este un standard 802.11 opțional, pentru criptare și autentificare, implementat în stratul MAC și pus la dispoziție de majoritatea producătorilor de NIC-uri radio și de puncte de acces. Atunci când instalați o rețea fără fir, trebuie să înțelegeți pe deplin capacitatea de a îmbunătăți securitatea rețelei oferită de WEP.

Funcționarea criptării WEP

Dacă utilizatorul activează WEP, placa de rețea radio criptează sarcina utilă — corpul cadrului și partea de verificare ciclică redundantă (în limba engleză: cyclic redundancy check — acronim CRC) — a fiecărui cadru 802.11, înainte de transmisie, folosind șirul de cifrare RC4 oferit de securitatea RSA². Stația receptoare, care poate fi un punct de acces sau o altă placă radio, efectuează decriptarea, după primirea cadrului. Prin urmare, metoda WEP pentru rețelele 802.11 criptează datele numai între stațiile 802.11. O dată ce cadrele ajung în partea cu fir a rețelei, cum ar fi între punctele de acces, WEP nu se mai aplică.

Ca parte a procesului de criptare, WEP pregătește un tabel cheie (germene) prin legarea cheii secrete partajate, furnizat de utilizatorul stației emițătoare, cu un vector de inițializare (în limba engleză: initialization vector — acronim IV) de 24 de biți, generat în mod aleator. Vectorul de inițializare prelungește viața cheii secrete, deoarece stația poate schimba vectorul de inițializare pentru fiecare transmisie de cadru. WEP introduce germenele rezultat într-un generator de numere pseudo-aleatoare care produce un șir cheie de lungime egală cu dimensiunea sarcinii utile a cadrului plus cei 32 de biți ai valorii de verificare a integrității (în limba engleză: integrity check value — acronim ICV)

ICV este o sumă de verificare pe care stația receptoare o recalculează și o compară cu cea transmisă de stația emițătoare. Astfel, determină dacă datele transmise au suferit modificări în timpul transferului. Dacă stația receptoare calculează o ICV care nu se potrivește cu cea găsită în cadru, aceasta îl poate respinge sau îl poate anunța pe utilizator.

WEP specifică o cheie secretă partajată pentru criptarea și decriptarea datelor. În cazul utilizării criptării WEP, stația receptoare trebuie să folosească aceeași cheie pentru decriptare. Prin urmare, fiecare placă de rețea radio și fiecare punct de acces trebuie să fie configurate manual cu aceeași cheie.

² RSA Data Security, Inc. este compania care a dezvoltat această metodă de criptare cu cheie publică (n. tr.),

Înainte să aibă loc transmisia, WEP combină șirul cheie cu sarcina utilă și cu valoarea de verificare a integrității printr-un proces OR exclusiv bit cu bit, care produce textul criptat (datele criptate). WEP include vectorul de inițializare (IV), în clar (necriptat), în primii biți ai corpului cadrului. Stația receptoare folosește acest IV împreună cu cheia secretă partajată furnizată de utilizatorul stației receptoare, pentru a decripta porțiunea sarcină utilă a corpului cadrului.

În majoritatea cazurilor, stația emițătoare va folosi vectori de inițializare diferiți pentru fiecare cadru (acest lucru nu este cerut de standardul 802.11). Atunci când sunt transmise mesaje care au un început comun, cum ar fi adresa expeditorului dintr-un mesaj e-mail, începutul fiecărei sarcini utile criptate va fi același atunci când se utilizează aceeași cheie. După criptarea datelor, începuturile cadrelor vor fi identice, oferind un tipar care îi poate ajuta pe hackeri să spargă algoritmul de criptare. Întrucât vectorii de inițializare sunt diferiți la majoritatea cadrelor, criptarea WEP asigură protecția împotriva acestui tip de atac. Schimbarea frecventă a IV-urilor îmbunătățește și capacitatea criptării WEP de a proteja împotriva periclitării datelor prin acțiunile cuiva.

Dezavantajele criptării WEP

WEP este vulnerabil datorită vectorilor de inițializare și cheilor relativ scurte care rămân neschimbate. Problema legată de WEP, nu are, de fapt, prea mare legătură cu algoritmul de criptare RC4. Având la dispoziție numai 24 de biți, WEP va folosi, în cele din urmă, același IV pentru pachete de date diferite. Pentru o rețea mare și aglomerată, această recurență a IV-ului se poate produce la un interval de timp de ordinul de mărime al unei ore.

Acest lucru conduce la transmiterea de cadre cu șiruri cheie care sunt prea asemănătoare. Dacă un hacker adună suficient de multe cadre bazate pe același IV, el va determina valorile partajate între cadre — ceea ce înseamnă că va afla șirul cheie sau cheia secretă partajată. Acest lucru îi va folosi hackerului la decriptarea oricărui cadru 802.11 din rețea.

Natura statică a cheilor secrete partajate accentuează această problemă. Standardul 802.11 nu oferă nici o funcție care să poată realiza schimbul de chei între stații. Prin urmare, administratorii de sisteme și utilizatorii folosesc, în general, aceleași chei timp de săptămâni, luni sau chiar ani. Acest lucru oferă răuvoitorilor suficient timp pentru a monitoriza și pentru a exploata rețelele cu criptare WEP activată.

Când trebuie folosită criptarea WEP

În ciuda punctelor sale slabe, trebuie să activați WEP ca un nivel minim de securitate. Multe persoane au descoperit rețelele fără fir care utilizează analizoare de protocol, cum ar fi AirPeek și AirMagnet. Majoritatea acestor persoane sunt capabile să detecteze rețelele fără fir în care criptarea WEP nu este utilizată iar apoi, folosind un laptop, să obțină accesul la resursele aflate în rețeaua asociată.

Totuși, prin activarea criptării WEP, veți micșora probabilitatea ca acest lucru să se întâmple, mai ales dacă aveți o rețea de locuință sau una de firmă mică. Criptarea WEP face o treabă bună, ținându-le la distanță pe majoritatea acestor persoane. Atenție însă! Prin preajmă există și hackeri adevărați care pot exploata slăbiciunile WEP și care pot accesa rețelele în care criptarea WEP este activată, mai ales pe acelea care sunt utilizate intens.

Protocolul de integritate cu cheie temporară

Standardul 802.11i include îmbunătățiri aduse securității LAN-urilor fără fir. Una dintre modernizări este protocolul de integritate cu cheie temporară (în limba engleză: Temporal Key Integrity Protocol — acronim TKIP), numit inițial WEP2. TKIP este o soluție interimară care rezolvă problema legată de reutilizarea cheii în criptarea WEP. De fapt, multe produse LAN fără fir au deja TKIP, ca o opțiune.

Procesul de criptare TKIP începe cu o cheie temporară de 128 de biți, partajată între clienți și punctele de acces. TKIP combină cheia temporară cu adresa MAC a clientului, iar apoi adaugă un IV relativ mare, de 16 octeți, pentru a produce cheia care va fi utilizată la criptarea datelor. Această procedură asigură faptul că fiecare stație folosește șiruri cheie diferite pentru a cripta datele.

Un avantaj al utilizării TKIP este acela că acele companii care au NIC-uri radio și puncte de acces bazate pe criptarea WEP pot să le modernizeze pentru trecerea la criptarea TKIP cu ajutorul unor pachete de software și hardware relativ simple. În plus, echipamentele care posedă doar criptarea WEP pot să interopereze, în continuare, cu dispozitivele care au inclusă criptarea TKIP, folosind WEP. TKIP constituie o soluție temporară, majoritatea experților considerând că este necesară o metodă de criptare mai puternică.

În afară de soluția TKIP, standardul 802.11i include protocolul numit standard de criptare avansată (în limba engleză: Advanced Encryption Standard — acronim AES). AES oferă o metodă de criptare mult mai puternică. AES utilizează algoritmul de criptare Rine Dale, o criptare extraordinar de puternică care înlocuiește algoritmul RC4. Majoritatea criptografilor consideră că AES nu poate fi spart. În plus, standardul 802.11i va include AES ca o opțiune peste TKIP. De fapt, organizația U.S. Commerce Department's National Institutes of Standard and Technology (NIST) a ales criptarea AES pentru a înlocui vechiul standard de criptare a datelor (în limba engleză: Data Encryption Standard — acronim DES). AES este acum un standard federal de procesare a informației, care definește un algoritm criptografic utilizat de organizațiile guvernamentale din SUA pentru protejarea informațiilor sensibile care nu sunt clasificate. Departamentul de comerț al guvernului SUA (Secretary of Commerce) a aprobat adoptarea AES, ca standard guvernamental oficial, în mai 2002.

Problema legată de utilizarea AES este aceea că acesta necesită o putere de procesare mai mare decât cea oferită de majoritatea punctelor de acces aflate astăzi pe piață. Prin urmare, implementarea AES va impune companiilor să-și modernizeze hardware-ul LAN fără fir existent pentru a putea asigura cerințele de performanță ale AES. Problema este că folosirea AES presupune funcționarea unui coprocesor (deci a unui hardware suplimentar). Aceasta înseamnă că firmele trebuie să-și înlocuiască punctele de acces și NIC-urile client existente pentru a implementa AES.

Accesul protejat Wi-Fi

Standardul numit accesul protejat Wi-Fi (în limba engleză: Wi-Fi Protected Access — acronim WPA) pus la dispoziție de Wi-Fi Alliance furnizează o modernizare a criptării WEP care oferă o criptare cu cheie dinamică și o autentificare reciprocă. Astăzi, majoritatea producătorilor includ WPA în produsele pentru rețele fără fir. Clienții WPA utilizează chei de criptare diferite care se schimbă periodic. Acest lucru face ca spargerea criptării să fie mai dificilă.

WPA 1.0 este, de fapt, o etapă a versiunii curente 802.11i, care include TKIP și mecanismele 802.1x. Combinația acestor două mecanisme oferă o criptare cu cheie dinamică și o autentificare reciprocă, lucruri de care LAN-uri fără fir aveau nevoie. Versiunea WPA 2.0 asigură o conformitate completă cu standardul 802.11i.

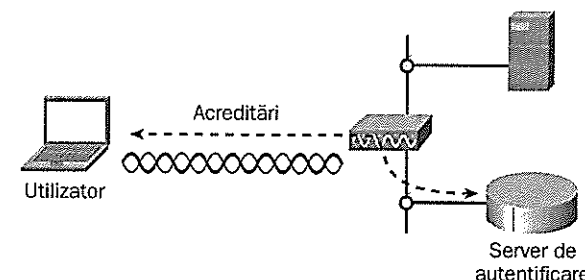
Rețele private virtuale

Dacă utilizatorii fără fir se deplasează în zone publice, cum ar fi aeroporturi și hoteluri, trebuie să luați în considerație soluțiile oferite de *rețeaua privată virtuală* (în limba engleză: *virtual private network* — acronim VPN). Chiar dacă VPN-urile nu sunt complet sigure, acestea oferă mijloace eficiente de criptare de la un capăt la celălalt al rețelei. De asemenea, VPN-urile sunt eficiente atunci când clienții se deplasează și întâlnesc diferite tipuri de rețele fără fir pentru că VPN-urile funcționează deasupra nivelelor conexiunilor de rețea, care sunt diferite.

Autentificarea

Într-o rețea fără fir, utilizarea autentificării reciproce este importantă. Această autentificare va păzi rețeaua de mai multe tipuri de amenințări la adresa securității, cum ar fi atacurile de tipul omul-la-mijloc. În cazul utilizării autentificării reciproce, clientul fără fir și rețeaua fără fir trebuie să-și dovedească reciproc identitatea. Acest proces utilizează un server de autentificare, cum ar fi Remote Authentication Dial-In User Service (RADIUS), pentru a realiza autentificarea. Figura 8.6 ilustrează procesul de autentificare.

Figura 8.6. Autentificarea verifică identitatea utilizatorilor și a dispozitivelor prin intermediul unor acreditări, cum ar fi parolele sau certificatele digitale



Punctele vulnerabile ale autentificării 802.11

Criptarea WEP oferă numai o metodă de autentificare a NIC-urilor radio față de punctele de acces, nu și în sens invers. Prin urmare, un hacker poate redirecționa datele pe o cale neautorizată, care evită alte mecanisme de securitate. În locul unei autentificări într-un singur sens, rețelele fără fir trebuie să implementeze o autentificare reciprocă pentru a evita o astfel de problemă.

Atunci când un client fără fir devine activ, el testează mediul în căutarea semnalelor far difuzate de punctele de acces. În mod obișnuit, semnalele far difuzate de punctele de acces conțin identificatorul setului de servicii (SSID) al punctului de acces, împreună cu alți parametri. Punctul de acces permite asocierea doar dacă SSID-ul clientului corespunde cu SSID-ul său. Acest proces oferă o formă de autentificare de bază, care este, însă, vulnerabilă.

Vulnerabilitatea majoră constă în faptul că SSID este transmis necriptat, ceea ce îl face vizibil pentru snifferele fără fir. Din această cauză, un hacker poate identifica cu ușurință SSID-ul din semnalul far și se poate autentifica în raport cu rețeaua fără fir. Chiar dacă punctul de acces este setat să nu difuzeze SSID-ul — o caracteristică opțională disponibilă doar la puține puncte de acces — snifferele pot totuși obține SSID-ul din cadrele de solicitare de asociere transmise de dispozitivele client către punctul de acces.

Standardul 802.11 oferă, în mod obișnuit, o formă de autentificare numită autentificarea sistemelor deschise. În acest mod de funcționare, punctul de acces acordă aprobarea oricărei solicitări de autentificare. Clientul trimite, pur și simplu, un cadru solicitare de autentificare, iar punctul de acces răspunde cu o aprobare de autentificare. Acest lucru permite ca oricine posedă SSID-ul corect să se asocieze la punctul de acces.

Standardul 802.11 include și o autentificare cu cheie partajată, o formă opțională, mai avansată, de autentificare. Aceasta este un proces în patru pași:

1. Clientul transmite un cadru solicitare de autentificare.
2. Punctul de acces răspunde cu un cadru care conține un șir de caractere numit text provocare.
3. Apoi, clientul criptează textul provocare folosind cheia comună de criptare WEP. Clientul transmite textul provocare criptat, înapoi la punctul de acces, care decriptează textul folosind cheia comună și compară rezultatul cu textul original transmis către client.
4. Dacă textul decriptat corespunde cu cel original, punctul de acces autentifică clientul.

Acest proces pare a fi potrivit pentru autentificare, însă există o problemă legată de faptul că autentificarea cu cheie partajată dovedește doar că respectivul client posedă cheia WEP corectă.

Filtrele MAC

Unele stații de bază fără fir oferă o filtrare prin controlul accesului la mediu (MAC). Atunci când se implementează filtrarea MAC, punctul de acces examinează adresa MAC sursă a cadrelor primite. Punctul de acces va respinge cadrele ale căror adrese sursă nu sunt cele dintr-o anumită listă programată de administratorul de rețea. Prin urmare, filtrarea MAC oferă o formă primitivă de autentificare.

Însă, filtrarea MAC are unele puncte slabe. De exemplu, WEP nu criptează câmpul adresei MAC din interiorul cadrului. Acest lucru permite unui hacker să monitorizeze cu ușurință transmisia cadrelor și să descopere astfel care sunt adresele MAC valide. Hackerul poate folosi un software disponibil gratuit pe piață, pentru a modifica adresele MAC ale NIC-urilor radio astfel încât acestea să corespundă unor adrese MAC valide. Acest lucru îi permite hackerului să se deghizeze într-un utilizator real și să înșele punctul de acces, atunci când utilizatorul legitim nu este prezent în rețea.

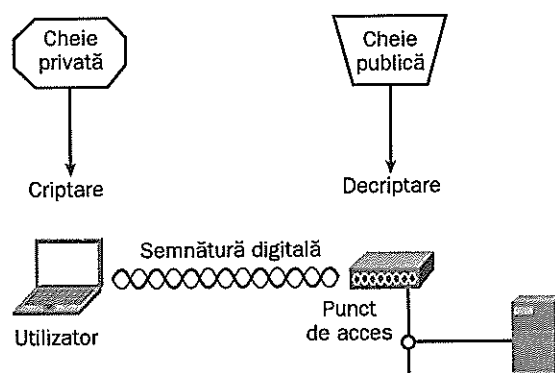
În plus, filtrarea MAC poate fi dificil de administrat atunci când există mulți utilizatori. Administratorul rețelei va trebui să introducă în tabel adresa MAC a fiecărui utilizator, iar apoi să facă modificările adecvate atunci când apar utilizatori noi. De exemplu, un angajat al companiei dintr-o altă locație poate avea nevoie să acceseze rețeaua locală fără fir pe parcursul vizitei sale la sediul central. Administratorul rețelei trebuie să determine adresa MAC a vizitatorului și să o programeze în sistem, înainte ca acesta să poată accesa rețeaua. Filtrarea adreselor MAC poate fi adecvată pentru aplicațiile de mici dimensiuni dedicate locuințelor sau sediilor de firme mici, însă faptul că această abordare necesită intervenții umane repetate o face indezirabilă în ochii administratorilor de rețele fără fir de întreprindere.

Autentificarea prin folosirea criptării cu cheie publică

Pe lângă faptul că protejează informațiile de hackerii, criptarea cu cheie publică poate fi utilizată de stații și pentru a se autentifica în raport cu alte stații sau în raport cu punctele de acces. Acest lucru poate fi necesar, înainte ca un punct de acces sau un controler să permită conectarea unei anumite stații la o parte protejată a rețelei. La fel, un client poate autentifica un punct de acces într-o manieră asemănătoare.

O stație se poate autentifica în raport cu o alta prin criptarea unui text dintr-un pachet, folosind cheia sa privată. Stația receptoare decriptează textul cu ajutorul cheii publice a stației emițătoare. Dacă textul decriptat este identic cu un text prestabilit, cum ar fi numele stației, stația receptoare va ști că stația emițătoare este validă. În acest caz, criptarea unui anumite porțiuni de text funcționează ca o semnătură digitală. Figura 8.7 ilustrează conceptul privitor la utilizarea criptării cu cheie publică pentru autentificare.

Figura 8.7. Criptarea cu cheie publică permite autentificarea



Standardul 802.1x

Utilizarea standardului IEEE 802.1x oferă un cadru eficient pentru autentificarea automată și pentru controlul traficului utilizatorilor dintr-o rețea protejată, precum și pentru criptarea cu cheie modificată dinamic. Standardul 802.1x combină protocolul numit protocol de autentificare extensibilă (în limba engleză: Extensible Authentication Protocol — acronim EAP), atât cu mediul de rețea fără fir, cât și cu cel de rețea cu fir și acceptă mai multe metode de autentificare, cum ar fi cardurile token, Kerberos, parolele de unică folosință, certificatele și autentificarea cu cheie publică.

Funcționarea 802.1x

Comunicarea 802.1x este inițiată de un solicitant (dispozitiv fără fir client) neautentificat, care încearcă să se conecteze la un autenticator (stație de bază fără fir). Stația de bază răspunde atribuind un port prin care să treacă numai pachetele EAP, transmise de la client la un server de autentificare, localizat în partea cu fir a rețelei conectate la stația de bază. Stația de bază blochează orice alt trafic, cum ar fi pachetele HTTP, DHCP și POP3, până când poate verifica identitatea clientului prin folosirea unui server de autentificare, cum ar fi RADIUS. O dată ce acesta este

autentificat, stația de bază deschide portul clientului pentru celelalte tipuri de trafic, în baza drepturilor de acces aflate pe serverul de autentificare.

Pentru a dobândi o idee mai exactă asupra modului în care se desfășoară procesul 802.1x, sunt enumerate în continuare interacțiunile specifice care se produc între diferitele elemente 802.1x:

1. Clientul transmite un mesaj EAP de inițiere. Acesta constituie începutul unei serii de mesaje schimbate pentru a se realiza autentificarea clientului; gândiți-vă la aceasta ca la situația în care un grup de vizitatori se află la intrarea într-un parc de distracții, iar conducătorul grupului (clientul) îl întreabă pe portar (stația de bază) dacă pot intra.
2. Stația de bază răspunde cu un mesaj EAP de solicitare de identitate. În cazul parcului de distracții, portarul îi va solicita conducătorului grupului numele său și permisul de conducere (cartea de identitate).
3. Clientul trimite către serverul de autentificare un pachet EAP de răspuns, care conține identitatea sa. Conducătorul grupului din exemplu îi comunică portarului numele său și îi înmânează permisul de conducere, iar acesta transmite aceste informații, mai departe, ghidului grupului (serverul de autentificare), care stabilește dacă grupul are dreptul de a intra.
4. Serverul de autentificare folosește un algoritm de autentificare specific pentru a verifica identitatea clientului. Această verificare se poate face prin intermediul certificatelor digitale sau printr-un alt tip de autentificare EAP. În exemplul nostru, procesul implică doar verificarea valabilității permisului de conducere al conducătorului grupului și confruntarea pozei din permis cu persoana respectivă. Să presupunem că respectivul conducător de grup este autorizat.
5. Serverul de autentificare va transmite un mesaj de acceptare sau de respingere la stația de bază. În cazul nostru, o acceptare înseamnă că ghidul parcului de distracții va spune portarului să lase grupul să intre.
6. Stația de bază transmite un pachet EAP de succes (al autentificării) la client. Portarul îl informează pe conducătorul grupului că grupul respectiv poate intra în parc. Bineînțeles că portarul nu va permite grupului să intre, dacă ghidul a respins solicitarea de acces a grupului.

7. Dacă serverul de autentificare îl acceptă pe client, stația de bază va trece portul clientului în starea autorizată și va retransmite restul traficului. Acest lucru este similar cu acțiunea portarului de a deschide poarta și de a lăsa să intre, în mod automat, numai persoanele care aparțin de grupul care a primit permisiunea de acces.

Protocolul de bază 802.1x furnizează o autentificare eficientă indiferent dacă implementați criptarea WEP 802.11 sau nici o altă criptare. Însă, cei mai mulți dintre producătorii de componente de rețele fără fir oferă versiuni brevetate de management bazat pe cheie dinamică folosind 802.1x ca un mecanism de livrare. Dacă este configurat să implementeze schimbul de chei dinamice, serverul de autentificare 802.1x poate returna chei de sesiune, la stația de bază, o dată cu mesajul de acceptare.

Stația de bază folosește cheile de sesiune pentru a construi, a marca și a cripta un mesaj EAP cheie, care este trimis la client imediat după transmiterea mesajului de succes (al autentificării). Apoi, clientul poate să folosească conținutul mesajului cheie pentru a defini chei de criptare adecvate. În implementările 802.1x tipice, clientul poate schimba automat și în mod frecvent cheile de criptare, pentru a minimiza riscul de a oferi curioșilor suficient timp pentru a sparge cheia aflată în uz.

Tipuri de autentificare

Este important să observați că standardul 802.1x nu oferă mecanismul efectiv de autentificare. Atunci când folosiți standardul 802.1x, va trebui să alegeți un tip de EAP — cum ar fi EAP Transport Layer Security (EAP-TLS), EAP Tunneled Transport Layer Security (EAP-TTLS) sau Lightweight EAP (LEAP) oferit de firma Cisco — care să definească modul în care se realizează autentificarea. Software-ul care implementează tipul respectiv de EAP este localizat pe serverul de autentificare și în sistemul de operare sau în software-ul de aplicație de pe dispozitivele clienților.

Politici de securitate

Unul dintre primii pași în asigurarea securității rețelei fără fir constă în formularea de politici eficiente și de procese de întărire a securității care să corespundă acestora. Analizați cu atenție cerințele de securitate și apelați la nivelurile de

protecție adecvate. De exemplu, criptarea trebuie să fie conținută în toate implementările de rețele fără fir. Criptarea WEP poate fi bună pentru rețelele instalate în locuințe sau în firme mici, dar trebuie să folosiți metode mai bune — cum ar fi WPA — pentru aplicațiile de corporație. O metodă de autentificare reciprocă eficientă — cum ar fi LEAP sau EAP-TLS — este, de asemenea, importantă pentru aplicațiile de corporație.

Etapele de evaluare a securității rețelei

După instalarea unei rețele fără fir, va trebui să realizați o evaluare a securității pentru a vă asigura că rețeaua locală fără fir respectă politicile de securitate stabilite. În majoritatea situațiilor, acest lucru este necesar dacă rețeaua implementează mecanisme de securitate eficiente. Nu vă bazați prea mult pe proiectarea sistemului. Cel mai bine este să efectuați teste pentru a vă asigura că rețeaua este suficient de întărită pentru a se proteja împotriva persoanelor neautorizate care pot ataca resursele companiei.

De fapt, companiile trebuie să realizeze revizuii regulate, periodice, ale securității pentru a se asigura că modificările apărute în rețeaua locală fără fir nu fac sistemul vulnerabil la hackeri. O revizie anuală poate fi suficientă pentru rețelele cu risc scăzut; însă, o revizie pe trimestru sau chiar mai des poate fi necesară dacă rețeaua vehiculează informații de mare risc, cum ar fi date financiare, direcționare de mesaje e-mail și funcții de control al producției.

Revizuirea politicilor de securitate existente

Înainte de a merge prea departe cu evaluările de securitate, familiarizați-vă cu politicile companiei referitoare la securitatea rețelei fără fir. Acest lucru oferă un nivel de referință pentru a stabili dacă o companie respectă propria politică de securitate. În plus, veți putea face evaluări și recomandări corespunzătoare pentru modificarea politicilor. Determinați dacă politicile lasă loc pentru ca un angajat nemulțumit să acceseze resursele companiei.

De exemplu, politica de securitate trebuie să descrie mecanismele de autentificare și criptare potrivite, pornind de la ideea că criptarea WEP 802.11 este spartă. De asemenea, politica trebuie să dispună ca toți angajații să se pună de acord cu departamentul IT al companiei, înainte de a achiziționa sau de a instala stații de

bază. Este important ca toate stațiile de bază să aibă setări de configurație care să fie în concordanță cu politicile și care să asigure un nivel de securitate adecvat. În plus, trebuie să vă asigurați că politicile de securitate sunt aduse la cunoștința angajaților într-un mod eficace.

Revizuirea sistemului existent

Întâlniți-vă cu personalul IT și citiți documentația legată de sistem pentru a înțelege arhitectura sistemului și configurările stațiilor de bază. Va trebui să determinați dacă există defecte de proiectare care constituie slăbiciuni pe care un hacker le poate exploata pentru a intra în sistem.

Învățați cât mai mult posibil despre instrumentele și procedurile existente pentru a identifica problemele potențiale. De exemplu, majoritatea companiilor configurează stațiile de bază printr-o magistrală cu fir Ethernet. În timpul acestui proces, parolele transmise pentru a deschide o conexiune cu o anumită stație de bază sunt trimise necriptat prin rețeaua cu fir. Prin urmare, un hacker care a atașat un echipament de monitorizare la rețeaua Ethernet va putea să captureze parolele și să reconfigureze stația de bază.

Discuțiile cu utilizatorii

Căutați să vorbiți cu un număr de angajați pentru a determina dacă aceștia cunosc politicile de securitate care îi privesc. De exemplu, știu aceștia că este necesar ca achiziționarea și instalarea de componente de rețea fără fir să fie coordonată de departamentul IT? Chiar dacă politicile de securitate stabilesc acest lucru, nu contați pe faptul că toată lumea le cunoaște. Cineva poate cumpăra o stație de bază de la un magazin local și o poate instala în rețeaua de corporație pentru a asigura conectivitatea fără fir dintr-un birou. De asemenea, este o idee bună să verificați dacă angajații folosesc parafocuri personale.

Verificarea configurațiilor dispozitivelor fără fir

Ca parte a evaluării, treceți prin zonele din sediu în care se află stații de bază și folosiți un instrument pentru a capta configurațiile acestora. Dacă compania a centralizat software-ul de asistență într-un singur loc, veți putea să verificați setările de configurare de la o singură consolă atașată la partea cu fir a rețelei. Veți face acest

lucru pentru a determina care sunt mecanismele de securitate care sunt efectiv utilizate și dacă acestea corespund unor politici eficace.

De exemplu, politica de securitate poate statua că stațiile de bază trebuie să aibă inactivat portul fizic de consolă, dar în cursul testării sesizați că majoritatea stațiilor de bază au porturile activate. Acest lucru va indica o nerespectare a politicilor și va permite unui hacker să reconfigureze stația de bază la setările prestabilite de fabrică care nu asigură securitatea. În plus, verificați versiunile hardware-ului și software-ului fiecărei stații de bază pentru a vedea dacă sunt actualizate. Versiunile mai vechi de software și hardware pot să nu implementeze pachetele mai recente care rezolvă vulnerabilitățile criptării.

De asemenea, investigați instalarea fizică a stațiilor de bază. Pe măsură ce vizitați sediul, verificați instalarea stațiilor de bază observând accesibilitatea lor fizică, tipul de antenă și orientarea acestora precum și propagarea undelor radio în acele zone ale sediului în care nu se pot face controale fizice de securitate. Stațiile de bază trebuie să fie montate în poziții care să facă dificilă manipularea lor de către cineva, fără ca persoana respectivă să fie observată.

De exemplu, plasarea unei stații de bază, pur și simplu, pe un raft cu cărți, va face ca înlocuirea acesteia, de către un hacker, cu o stație pirat care nu are activate mecanisme de securitate, să fie ușor de realizat. Sau, hackerul poate conecta un laptop la portul consolă pentru a reconfigura stația de bază. Dacă, însă, stațiile de bază sunt toate montate deasupra tavanului fals și în afara razei vizuale, hackerul va trebui să folosească o scară și va fi probabil observat de un angajat sau de cineva din serviciul de pază.

Identificarea stațiilor de bază pirat

O problemă o constituie faptul că securitatea unei rețele este dificil de întărit atunci când un angajat instalează o stație de bază personală în biroul său, afectând semnificativ securitatea rețelei. În majoritatea cazurilor, aceste instalări nu respectă politicile de securitate și oferă un port de intrare deschis, neprotejat în rețeaua de corporație. De fapt, un hacker poate utiliza instrumente de monitorizare care să îl alerteze dacă există astfel de oportunități.

Prin urmare, scanați pentru a identifica aceste stații de bază neautorizate, ca o parte a procesului de evaluare. Majoritatea companiilor vor fi surprinse să afle câte lucruri neașteptate vor găsi. Cea mai eficientă metodă de depistare a stațiilor de bază pirat este să vă deplasați prin sediu cu un instrument de monitorizare. În plus, compania va trebui să scaneze periodic rețeaua pentru depistarea stațiilor de bază pirat din partea cu fir a rețelei. Această posibilitate este oferită de multe sisteme de management centralizat al rețelelor fără fir.

Realizarea de teste de penetrare

În afară de vânarea stațiilor de bază pirat, încercați să faceți un pas înainte și probați accesarea resurselor companiei folosind instrumentele obișnuite aflate la dispoziția hackerilor. De exemplu, puteți folosi AirSnort pentru a sparge criptarea WEP? Este posibil să vă asociați cu o stație de bază atunci când vă aflați în afara perimetrului controlat al companiei? Bineînțeles că această sarcină va fi mai ușoară dacă criptarea WEP nu este activă. Dacă sunt utilizate tehnici puternice de criptare și de autentificare, probabil că nu veți reuși să accesați rețeaua.

Analiza lacunelor sistemului de securitate

Informațiile pe care le adunați în timpul procesului de evaluare oferă o bază pentru a înțelege starea de securitate a companiei sau a organizației. După colectarea informațiilor, acordați-vă ceva timp pentru a vă gândi la lacunele potențiale ale sistemului de securitate. Aceasta include aspecte legate de politici, de arhitectura rețelei, de asistența în funcționare și de alte chestiuni care pot slăbi securitatea, cum ar fi prezența unor stații de bază neautorizate și capacitatea de penetrare a rețelei. Acest lucru vă cere să gândiți ca un hacker și să descoperiți toate metodele care fac ca cineva să poată penetra rețeaua și să poată accesa (sau controla) cu mai mare ușurință resursele companiei prin intermediul rețelei fără fir.

Recomandarea de îmbunătățiri aduse securității

Pe măsură ce identificați slăbiciunile, cercetați și descrieți metodele care vor rezolva aceste probleme. Începeți prin a recomanda îmbunătățiri ale politicilor de securitate, care dictează care sunt cerințele companiei în materie de securitate a rețelei fără fir. Acest lucru oferă o bază pentru definirea de soluții tehnice și procedurale care să întărească sistemul de securitate până la nivelul la care se realizează protejarea intereselor companiei.

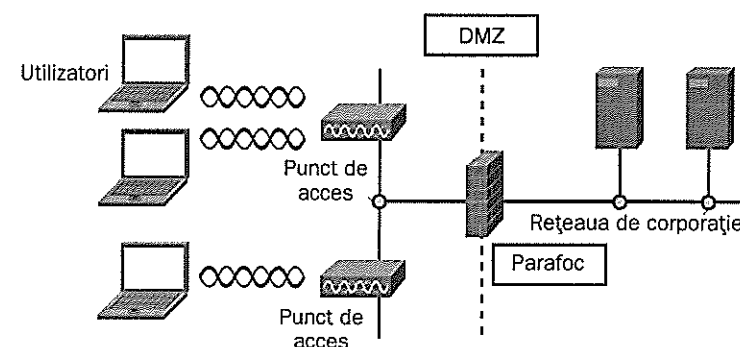
Politici de securitate uzuale

Indiferent despre ce rețea fără fir este vorba, trebuie luate în considerație politici care vor proteja resursele în raport cu persoanele neautorizate. Să vedem ce ar trebui să includă astfel de politici.

Plasarea utilizatorilor fără fir în exteriorul unui parafoc

Luați în considerare realizarea unei zone demilitarizate (în limba engleză: demilitarized zone — acronim DMZ) fără fir prin plasarea unui parafoc între rețeaua fără fir și rețeaua de corporație (vezi figura 8.8). În cazul acestei abordări, echipați fiecare dispozitiv de utilizator cu o rețea privată virtuală (VPN), pe care rețeaua protejată o va accepta. În consecință, un hacker va trebui să utilizeze o VPN configurată în mod corect — lucru dificil de făcut — pentru a obține accesul la resursele companiei.

Figura 8.8. Parafocurile oferă protecție suplimentară rețelelor fără fir



Problema generată de folosirea VPN-urilor pentru fiecare utilizator este aceea că sunt dificil de administrat și uneori reduc performanțele rețelei. Prin urmare, aveți în vedere această soluție mai ales dacă utilizatorii se vor deplasa prin spații publice.

Utilizarea unei criptări eficiente

Hackerii experimentați pot penetra rețelele protejate prin criptarea WEP utilizând instrumente disponibile gratuit. Totuși, criptarea WEP face o treabă bună protejând multe rețele de locuință sau de firmă față de publicul larg. Pentru a sparge criptarea WEP, trebuie să știți cum să folosiți instrumente complicate și trebuie să capturați un număr mare de pachete din rețea, un lucru cu care majoritatea oamenilor nu-și vor

pierde timpul decât dacă resursele rețelei sunt extrem de valoroase și dacă au foarte multă răbdare. Utilizarea standardului 802.11 WEP pentru rețelele cu risc scăzut de atac este o cerință minimală a oricărei politici de securitate.

Dacă hardware-ul rețelei dumneavoastră fără fir acceptă o formă de criptare care schimbă frecvent cheile (cum ar fi WPA), folosiți-o. Acest lucru oferă o soluție mult mai sigură decât utilizarea metodelor statice, cum este criptarea WEP. Dacă sunt necesare măsuri de securitate foarte înaltă, utilizați standarde superioare, cum ar fi AES.

Asigurați-vă că software-ul și hardware-ul sunt actualizate

Adesea producătorii implementează „petice” la software-ul stațiilor de bază și al NIC-urilor radio pentru a repara hibe de securitate. Începeți să actualizați software-ul/hardware-ul stațiilor de bază curând după ce le instalați. Faceți-vă un obicei din verificarea periodică a faptului că toate dispozitivele au cele mai recente software-uri/hardware-uri lansate pe piață pentru a acoperi toate lacunele de securitate cunoscute. De aceea, este o idee bună să vă asigurați că puteți moderniza cu ușurință software-ul/hardware-ul stațiilor de bază pe care le cumpărați.

Protejarea fizică a stațiilor de bază

Unele stații de bază se vor reîntoarce la configurările prestabilite de fabrică, care nu asigură nici un fel de protecție, atunci când cineva apasă un buton de repornire. Acest lucru face ca stația de bază să fie un punct de intrare fragil. Prin urmare, asigurați o protecție fizică adecvată pentru hardware-ul stațiilor de bază.

De exemplu, nu plasați o stație de bază într-un loc ușor accesibil ca un birou dintr-o încăpere. În schimb, montați-le în afara razei de vedere, deasupra tavanului fals. Unele stații de bază nu au butoane de repornire, dar vă permit să le reconfigurați prin intermediul unui cablu RS-232 conectat la o consolă. Pentru a preveni o astfel de reconfigurare, asigurați-vă că portul de consolă este dezactivat.

De asemenea, nu lăsați stațiile de bază în zone în care poate ajunge un hacker, care poate înlocui o stație de bază legitimă, protejată, cu o stație de bază pirat, fără protecție, care acceptă accesul oricărui utilizator. De fapt, este o idee bună să ascundeți, pe cât posibil, stațiile de bază pentru a le face greu de găsit de către un hacker. Asigurați-vă, însă, că ați notat locațiile hardware-urilor fără fir; altfel, s-ar putea să aveți dificultăți să le regăsiți chiar și dumneavoastră.

Dezactivați stațiile de bază în perioadele în care rețeaua nu e utilizată. Dacă este posibil, opriți stațiile de bază atunci când utilizatorii nu au nevoie de ele. Acest lucru limitează oportunitățile pentru un hacker. Puteți decupla alimentarea fiecărei stații de bază; însă, puteți avea în vedere instalarea unor echipamente Power-over-Ethernet (vezi pagina 47) care asigură această posibilitate prin instrumente de asistență centralizată în funcționare.

Atribuiți parole puternice pentru stațiile de bază

Nu utilizați parolele prestabilite ale stațiilor de bază. Parolele prestabilite sunt bine cunoscute, de aceea cineva poate realiza cu ușurință schimbarea parametrilor de configurare a stațiilor de bază, în avantajul său. În schimb, folosiți parole care sunt dificil de ghicit. De fapt, este o idee bună să utilizați un amestec de majuscule și litere mici combinate cu simboluri speciale. Asigurați-vă că aceste parole sunt modificate periodic. De asemenea, asigurați-vă că parolele sunt criptate înainte de a fi transmise prin rețea.

Evitați difuzarea SSID-urilor

Dacă utilizarea SSID este disponibilă, puteți evita să aveți în rețea dispozitive de utilizator care să monitorizeze, în mod automat, SSID-urile folosite de punctele de acces ale unei LAN fără fir. Windows XP și alte instrumente de monitorizare vor sesiza automat cădrele far 802.11 pentru a obține SSID-ul. Dezactivând difuzarea SSID-urilor, stația de bază nu va mai include SSID-ul în cadrul far, ceea ce face ca majoritatea instrumentelor de monitorizare să fie inutile. În plus, utilizatorii de Windows și de Windows XP nu vor mai sesiza existența rețelei locale fără fir.

Dezactivarea difuzării SSID-urilor nu este, însă, o metodă complet sigură, deoarece cineva poate, în continuare, să monitorizeze cadrele 802.11 de asociere și astfel să obțină SSID-ul. Dezactivarea mecanismului de difuzare va limita, totuși, accesul.

Limitarea propagării undelor radio

Prin utilizarea antenelor direcționale, este posibil să se limiteze propagarea undelor radio la o zonă în care hackerii nu pot avea acces fizic. De exemplu, proiectul unei rețele fără fir poate specifica câștigul și orientarea unei antene pentru a reduce împrăștierea undelor radio în afara perimetrului unui sediu. Acest lucru, nu

numai că va optimiza acoperirea rețelei, dar va și minimiza capacitatea unui curios de a intercepta transmisia semnalului unui utilizator sau de se conecta la rețeaua de corporație, printr-un punct de acces.

Implementarea de parafocuri personale

Dacă un hacker poate să se asocieze la o stație de bază, el va putea să acceseze, cu ușurință, fișierele de pe alte dispozitive de utilizator, care sunt asociate la un punct de acces conectat la aceeași rețea LAN fără fir, prin intermediul sistemului de operare Windows. Prin urmare, este crucial ca toți utilizatorii să dezactiveze partajarea fișierelor din toate dosarele și să utilizeze parafocurile personale. Acest lucru este foarte important atunci când utilizatorii funcționează în locații publice.

Monitorizarea configurației stațiilor de bază

Utilizați instrumente pentru asistență în funcționare pentru a monitoriza, în permanență, rețeaua și pentru a verifica dacă există stații de bază care nu se conformează politicilor de configurare. O stație de bază care nu corespunde configurărilor de securitate specifice probabil că a fost reconfigurată sau este posibil să fie o stație de bază pirat.

Dacă sunt găsite stații de bază cu configurări improprii, refaceți configurările cât mai curând posibil. Asigurați-vă, însă, că traficul de administrare este criptat, prin folosirea unei versiuni sigure a protocolului numit Simple Network Management Protocol (SNMP). SNMP versiunea 1, de exemplu, transmite toate datele în clar. Puteți să instalați și senzori pentru detectarea intruziunilor, disponibili la anumite instrumente pentru asistență în funcționare, pentru a identifica prezența hackerilor pe baza adreselor MAC nevalide. Ideea de bază este să asigurați alertarea în cazul în care sunt sesizate comportamente care stârnesc suspiciuni.

Desfășurarea de controale

Asigurați-vă că toți angajații și organizațiile din companie coordonează instalarea rețelelor fără fir prin grupul IT adecvat. De exemplu, interziceți utilizarea de puncte de acces neautorizate. Dispuneți utilizarea produselor unor producători agreeți, după ce ați avut posibilitatea de a verifica protecțiile de securitate adecvate puse la dispoziție de acestea.

Păstrați o listă de adrese MAC pentru NIC-uri radio și stații de bază autorizate, pe care o puteți folosi în timpul supravegheților rețelei, ca bază pentru identificarea stațiilor de bază pirat. În plus, instalați instrumente de administrare care forțează stațiile de bază să respecte politicile de securitate ale corporației.

Având în minte aceste recomandări, posedați bazele necesare alcătuirii unei politici de securitate solide. Atunci când decideți ce tehnică veți implementa, luați în considerare nevoile reale de securitate. De exemplu, criptarea WEP poate fi suficient de bună pentru LAN-urile fără fir dedicate locuințelor și firmelor mici. Dacă lucrați pentru o instituție financiară sau pentru un magazin de comerț cu amănuntul și transmiteți date importante, concentrați-vă pe folosirea unor metode mai puternice, cum ar fi WPA sau AES.

Rezumatul capitolului

Securitatea este unul dintre cele mai importante și complexe aspecte ale rețelelor fără fir. Posibilitatea unui hacker de a monitoriza traficul, de a obține accesul neautorizat la resurse valoroase și de a realiza atacuri negare de serviciu într-o rețea fără fir, sunt elemente pe care trebuie să le luați în considerație. Prin folosirea unei autentificări și a unei criptări eficiente, este posibil să reduceți semnificativ amenințările la adresa securității. Rețineți, însă, că nivelul de securitate necesar depinde de cerințe. Un nivel de securitate acceptabil pentru o aplicație destinată unei locuințe este mult mai scăzut decât cel necesar pentru o rețea de întreprindere.

Întrebări recapitulative

Puteți găsi răspunsurile la întrebările următoare în Anexa A, intitulată *Răspunsuri la întrebările recapitulative*.

1. Care sunt cele trei amenințări majore la adresa securității rețelelor fără fir?
2. Care este mijlocul principal de protecție împotriva monitorizării traficului?
3. Cum îi puteți împiedica pe hackeri să obțină accesul la resursele companiei prin intermediul rețelei fără fir?

4. Care este metoda care vă poate ajuta să limitați implicațiile unui atac DoS reușit?
5. De ce criptarea WEP nu este acceptabilă pentru protejarea informațiilor importante?
6. Prin ce diferă TKIP de criptarea WEP?
7. WPA utilizează TKIP și este un subset al standardului 802.11i. Adevărat sau fals?
8. De ce utilizarea filtrării adreselor MAC nu este eficace?
9. Ce este un punct de acces pirat și de ce generează acesta probleme într-o rețea fără fir?
10. Ce trebuie instalat pe un laptop care urmează să fie folosit de un utilizator într-o LAN fără fir publică, pentru a se evita accesarea fișierelor de pe laptop de către persoane neautorizate?

Răspunsuri la întrebările recapitulative

Capitolul 1

1. Care este atributul distinctiv al unei rețele fără fir prin comparație cu un sistem general de comunicații fără fir?

Răspuns: Într-o rețea fără fir, comunicațiile se realizează între dispozitivele de calcul.

2. Care sunt tipurile de informații a căror transmisie poate fi asigurată de o rețea fără fir?

Răspuns: Mesaje e-mail, mesaje text, pagini Web, înregistrări de baze de date, secvențe video și de voce.

3. Care sunt cele patru tipuri de rețele fără fir?

Răspuns: PAN-urile, LAN-urile, MAN-urile și WAN-urile fără fir.

4. Care este raza de acțiune maximă obișnuită a unei rețele PAN fără fir?

Răspuns: 17 metri (50 de pași).

5. Adevărat sau fals: O rețea PAN fără fir consumă o putere scăzută de la micile dispozitive de calcul de mână.

Răspuns: Adevărat.

6. Care sunt standardele uzuale pentru LAN-urile fără fir?

Răspuns: IEEE 802.11 și Wi-Fi.



7. Care este standardul relativ nou care se aplică la MAN-urile fără fir?

Răspuns: IEEE 802.16.

8. Care este motivul pentru care WAN-urile fără fir nu satisfac, în mod eficient, cerințele pentru rețelele fără fir, în interiorul clădirilor?

Răspuns: Sistemele WAN fără fir sunt instalate, în general, în exteriorul clădirilor, iar semnalele își pierd din putere înainte de a ajunge în interiorul clădirilor.

9. Care este aplicația uzuală a rețelelor fără fir în locuințe și în sediile de firme mici?

Răspuns: O aplicație uzuală este partajarea conexiunilor la Internet între mai multe calculatoare mobile.

10. Care sunt exemplele de aplicații ale WAN-urilor fără fir?

Răspuns: Aplicații de accesare a Internetului din locații exterioare, tranzacții imobiliare, servicii legate de activitățile de teren și de vânzări pe teren, starea automatelor pentru vânzări și măsurarea consumurilor de utilități sunt câteva exemple.

Capitolul 2

1. Care sunt factorii de formă cei mai potriviți pentru NIC-urile fără fir utilizate pentru dispozitivele de calcul fără fir de dimensiuni mici?

Răspuns: Placă PC, Mini-PCI și CompactFlash (CF).

2. Care sunt exemplele de fenomene atmosferice care afectează propagarea semnalelor de comunicații fără fir prin mediul aerian?

Răspuns: Ploaia, ninsoarea, smogul și fumul.

3. Care este scopul principal al unei stații de bază?

Răspuns: Realizarea unei interfețe cu o rețea cu fir, pentru semnalele de comunicații fără fir care călătoresc prin mediul aerian.

4. Care sunt caracteristicile comune ale unui middleware fără fir?

Răspuns: Tehnici de optimizare, reporniri inteligente, comasarea de date, modificarea configurației ecranelor, asistarea sistemelor finale.

5. În ce straturi ale modelului de referință OSI operează rețelele fără fir?

Răspuns: În stratul fizic și în stratul legătură de date.

6. Prin ce diferă transferul de viteză de transmisie a datelor?

Răspuns: Transferul nu include surplusul adăugat de protocoale peste datele utilizatorului.

7. Adevărat sau fals: Un dispozitiv de calcul stochează datele în formă analogică.

Răspuns: Fals.

8. În ce fel de tip de semnal trebuie convertită informația, de către o placă NIC fără fir, înainte de a fi transmisă prin mediul aerian?

Răspuns: În tipul de semnal analogic.

9. Care este protocolul uzual pentru accesul la mediu folosit de rețelele fără fir?

Răspuns: CSMA (accesul multiplu cu sesizarea purtătoare).

10. Explicați cum realizează ARQ controlul erorilor de transmisie.

Răspuns: Placa de rețea fără fir receptoare realizează verificarea erorilor și, dacă descoperă erori în cadru, trimite o solicitare de retransmitere a acestuia, la placa de rețea fără fir emițătoare.

Capitolul 3

1. Semnalele RF asigură o rază de acțiune relativ scurtă prin comparație cu semnalele luminoase. Adevărat sau fals?

Răspuns: Fals.

2. Ce tipuri de condiții meteo afectează cel mai mult semnalele RF?

Răspuns: Ploile torențiale.



3. De ce interferențele produc erori în rețelele fără fir?

Răspuns: Interferențele fac ca receptorul să nu înțeleagă semnalul datorită faptului că sunt prezente simultan două semnale.

4. Care sunt sursele interferențelor RF?

Răspuns: Exemplele generale includ telefoanele fără fir, cuptoarele cu microunde și dispozitivele Bluetooth.

5. Propagarea pe căi multiple afectează mai mult sistemele de frecvență 2,4 GHz cu viteze de transmisie a datelor mai mari decât pe cele cu viteze de transmisie a datelor mai mici. Adevărat sau fals?

Răspuns: Adevărat. Receptorul are dificultăți să diferențieze un bit de un altul atunci când demodulează semnale cu viteze de transmisie a datelor mari, deoarece biții sunt foarte apropiați unul de celălalt.

6. Ce se înțelege prin sistem cu lumină infraroșie difuză?

Răspuns: Un sistem care emite lumină infraroșie în toate direcțiile, lumină care se reflectă apoi de tavane și pereți.

7. Care este raza de acțiune aproximativă a sistemelor care operează cu lumină infraroșie directă?

Răspuns: 1,6 km (1 milă).

8. Ce face modularea astfel încât să fie posibilă transmiterea informațiilor prin aer?

Răspuns: Modularea suprapune un semnal de informație pe un semnal purtător care are o frecvență potrivită pentru propagarea prin aer.

9. Care sunt caracteristicile unui semnal pe care QAM le modifică pentru a realiza reprezentarea informațiilor?

Răspuns: Amplitudinea și faza.

10. În general, spectrul larg necesită licență de utilizator. Adevărat sau fals?

Răspuns: Fals.

Capitolul 4

1. Care sunt factorii de formă obișnuiți ai plăcilor radio pentru PAN-uri fără fir?

Răspuns: Placă PC și CF (CompactFlash).

2. Care sunt aplicațiile care pot obține avantaje importante de pe urma utilizării unui adaptor USB fără fir (numit și cheie fără fir)?

Răspuns: Orice aplicație care poate beneficia de pe urma realizării unei interfețe cu un PC sau un laptop printr-un port USB, cum ar fi un PDA, un mouse fără fir, o cameră digitală fără fir conectate în scopul sincronizării.

3. Când are sens să fie utilizate routerele PAN fără fir?

Răspuns: Pentru aplicații limitate la dimensiunile unei încăperi, cum sunt cele pentru o locuință sau pentru un sediu mic de firmă.

4. Care este aria de acoperire maximă obișnuită a PAN-urilor fără fir?

Răspuns: Până în 10 metri distanță, adică în interiorul unei încăperi.

5. Care este grupul de standarde IEEE care utilizează specificația Bluetooth ca bază pentru standardul respectiv?

Răspuns: 802.15.

6. În ce bandă de frecvență operează Bluetooth?

Răspuns: 2,4 GHz.

7. Care este principala problemă ridicată de funcționarea Bluetooth în apropierea LAN-urilor fără fir 802.11?

Răspuns: Ambele sisteme funcționează în banda de frecvență de 2,4 GHz, ceea ce poate conduce la producerea de interferențe și de aici la scăderea performanțelor.

8. Un dispozitiv care are capacitate Bluetooth transmite în permanență. Adevărat sau fals?

Răspuns: Fals.

9. Care este viteza de transmisie a datelor cea mai ridicată posibilă pentru un dispozitiv IrDA?

Răspuns: 4 Mbps.

10. Care este avantajul utilizării IrDA prin comparație cu Bluetooth?

Răspuns: Sistemele IrDA sunt imune la interferențele RF produse datorită LAN-urilor fără fir.

Capitolul 5

1. Care este componenta LAN fără fir cel mai des folosită în locuințe și în sediile firmelor mici?

Răspuns: Routerul LAN fără fir.

2. Care este principala diferență dintre un punct de acces și un router LAN fără fir?

Răspuns: Un router LAN fără fir direcționează, de fapt, pachetele la destinațiile acestora. Punctele de acces nu implementează DHCP și NAT. În schimb, routerele implementează DHCP și NAT.

3. Când are sens să fie utilizat un repetor LAN fără fir?

Răspuns: Atunci când se dorește extinderea razei de acțiune a unui punct de acces sau a unui router într-o zonă în care instalarea de cabluri nu este realizabilă.

4. Cum identifică o placă NIC radio pentru LAN-uri fără fir punctul de acces cu care să se asocieze?

Răspuns: Placa de rețea radio ascultă mediul în căutarea semnalelor far care sunt transmise periodic de fiecare punct de acces și se asociază cu acel punct de acces care are cel mai puternic semnal far.

5. WEP este un mecanism de criptare obligatoriu. Adevărat sau fals?

Răspuns: Fals.

6. Care este banda de frecvență în care funcționează rețelele 802.11a?

Răspuns: 5 GHz.

7. Câte canale de transmisie, care nu se suprapun, sunt disponibile într-o rețea LAN fără fir 802.11b?

Răspuns: Trei.

8. Adevărat sau fals: rețelele 802.11g funcționează la viteze de transmisie a datelor de până la 54 Mbps și sunt interoperabile cu rețelele 802.11b.

Răspuns: Adevărat.

9. Care dintre frecvențele specificate de standardul 802.11 este disponibilă aproape oriunde în lume?

Răspuns: 2,4 GHz (rețele 802.1b și 802.11g).

10. Ce oferă certificarea Wi-Fi?

Răspuns: Un produs care este certificat Wi-Fi va fi interoperabil cu alte produse care sunt certificate Wi-Fi, indiferent de fabricanții acestora.

Capitolul 6

1. De ce instalarea MAN-urilor fără fir asigură beneficii bune în urma investiției?

Răspuns: MAN-urile fără fir elimină necesitatea instalării unor cabluri scumpe sau necesitatea închirierii unor circuite de comunicații.

2. O punte care învață retransmite toate pachetele primite. Adevărat sau fals?

Răspuns: Fals.

3. Care este diferența principală dintre o punte și un punct de acces?

Răspuns: O punte conectează rețele. Un punct de acces conectează utilizatori finali.

4. Care sunt exemplele de antene semidirecționale prezentate în acest capitol?

Răspuns: Antena cu fâșie direcțională (în limba engleză: directional patch antenna) și antena Yagi.

5. Care este diferența principală dintre o antenă semidirecțională și una de mare directivitate, din punctul de vedere al lățimii de lob?

Răspuns: O antenă de mare directivitate are o lățime de lob mult mai îngustă, ceea ce duce la creșterea razei de acțiune, dacă puterea de emisie rămâne constantă.

6. Dați un exemplu de antenă de mare directivitate.

Răspuns: Antena parabolică.

7. Care este cea mai eficace polarizare a unei antene receptor, dacă emițătorul folosește polarizarea verticală?

Răspuns: Polarizarea verticală.

8. Care sunt avantajele utilizării unui sistem punct-la-multe-puncte, prin comparație cu sistemele punct-la-punct, în cazul interconectării mai multor locații?

Răspuns: Sistemele punct-la-multe-puncte pot fi mai ieftine și permit, cu ușurință, adăugarea de noi locații.

9. Care sunt avantajele utilizării sistemelor radio cu pachete pentru MAN-urile fără fir?

Răspuns: Routerile pentru pachete radio nu necesită nici un fel de cabluri între ele, iar sistemul funcționează chiar dacă unele routere nu mai sunt operaționale, deoarece pachetele de date pot urma rute diferite, care să evite aceste routere.

10. Care sunt standardele folosite de MAN-urile fără fir?

Răspuns: 802.11, Wi-Fi și 802.16.

Capitolul 7

1. Care sunt cele mai comune tipuri de dispozitive pentru utilizatorii WAN-urilor fără fir?

Răspuns: Laptopurile, PDA-urile și telefoanele mobile.

2. De ce operatorii de WAN-uri fără fir taxează întotdeauna serviciile oferite?

Răspuns: Pentru că instalarea WAN-urilor fără fir este scumpă.

3. De ce trebuie să fiți atent atunci când alegeți o placă NIC radio WAN fără fir pentru dispozitivul dumneavoastră de utilizator?

Răspuns: Pentru că există multe tipuri diferite de WAN-uri fără fir care nu sunt compatibile între ele.

4. Care este unul dintre avantajele utilizării unui sistem bazat pe satelit?

Răspuns: Un sistem bazat pe satelit poate acoperi suprafețe vaste. Un singur satelit geostaționar poate acoperi, în mare, o treime din suprafața Pământului.

5. Ce generație de sisteme celulare oferă viteze de transmisie a datelor de până la 2 Mbps?

Răspuns: A treia generație (3G).

6. Care este cel mai comun tip de sistem WAN fără fir?

Răspuns: Sistemul celular.

7. Care dintre următoarele două tipuri de sisteme celulare oferă viteze de transmisie a datelor mai mari: GPRS sau UMTS?

Răspuns: UMTS.

8. Care este principala problemă legată de comunicațiile bazate pe reflexia undelor radio pe stratul de gaze ionizate produse de arderea meteorilor?

Răspuns: Viteza scăzută de transmisie a datelor.

9. Adevărat sau fals: FDMA solicită utilizatorilor să își aștepte rândul pentru a-și transmite semnalele.

Răspuns: Fals.

10. Cum evită CDMA posibilitatea ca utilizatorii să-și producă, unul altuia, interferențe?

Răspuns: Fiecare utilizator transmite folosind un alt cod.

Capitolul 8

1. Care sunt cele trei amenințări majore la adresa securității rețelelor fără fir?

Răspuns: Monitorizarea traficului, accesul neautorizat și atacul negare de serviciu (DoS).

2. Care este mijlocul principal de protecție împotriva monitorizării traficului?

Răspuns: Utilizarea criptării.

3. Cum îi puteţi împiedica pe hackeri să obţină accesul la resursele companiei prin intermediul reţelei fără fir?

Răspuns: Prin utilizarea unui mecanism de autentificare eficace.

4. Care este metoda care vă poate ajuta să limitaţi implicaţiile unui atac DoS reuşit?

Răspuns: Trebuie să aveţi un plan alternativ pentru continuarea funcţionării firmei într-un mod care să nu presupună folosirea reţelei fără fir.

5. De ce criptarea WEP nu este acceptabilă pentru protejarea informaţiilor importante?

Răspuns: Hackerii pot sparge algoritmul de criptare WEP cu ajutorul unor instrumente disponibile public.

6. Prin ce diferă TKIP de criptarea WEP?

Răspuns: TKIP foloseşte un mecanism de distribuţie cu cheie dinamică care actualizează cheile periodic, în timp ce criptarea WEP foloseşte chei statice care nu sunt schimbate.

7. WPA utilizează TKIP şi este un subset al standardului 802.11i. Adevărat sau fals?

Răspuns: Adevărat.

8. De ce utilizarea filtrării adreselor MAC nu este eficace?

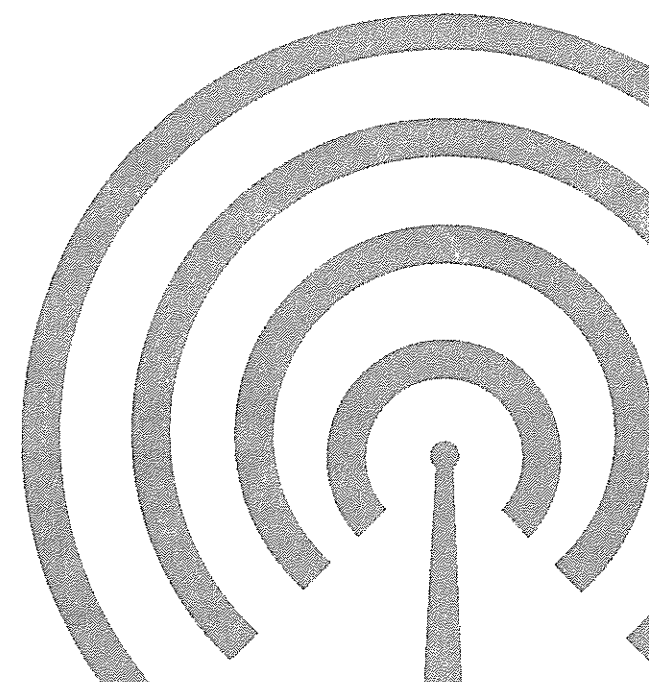
Răspuns: Filtrarea adreselor MAC este un mecanism dificil de administrat şi uşor de înşelat.

9. Ce este un punct de acces pirat şi de ce generează acesta probleme într-o reţea fără fir?

Răspuns: Un punct de acces pirat nu are configurate nici un fel de caracteristici de securitate şi este instalat în reţea de către un hacker sau un angajat al firmei care posedă reţeaua respectivă. Punctul de acces pirat oferă un port deschis către reţea pe care hackerii îl pot exploata.

10. Ce trebuie instalat pe un laptop care urmează să fie folosit de un utilizator într-o reţea LAN fără fir publică, pentru a se evita accesarea fişierelor de pe laptop de către persoane neautorizate?

Răspuns: Un parafoc personal.



Glosar

802.11 Standard publicat de IEEE care definește caracteristicile radio și modul de funcționare ale LAN-urilor de radio frecvență cu rază medie de acțiune.

802.15 Standard publicat de IEEE care definește caracteristicile radio și modul de funcționare ale PAN-urilor fără fir. 802.15 este bazat pe specificația Bluetooth.

802.16 Standard publicat de IEEE care definește caracteristicile radio și modul de funcționare ale MAN-urilor fără fir.

802.3 Standard publicat de IEEE care definește caracteristicile semnalului și modul de funcționare ale rețelelor locale cu fir.

acces cu sesizarea purtătoarei Proces de partajare a unui mediu comun care începe prin a determina dacă mediul este disponibil, înainte de transmiterea datelor. Face parte din protocolul CSMA.

acces la mediu Proces prin care mai multe dispozitive de calcul își împart (partajează) un mediu comun. Cea mai comună metodă de acces la mediu pentru rețele fără fir este CSMA.

acces multiplu cu divizare prin cod *vezi* CDMA.

acces multiplu cu urmărirea purtătoarei *vezi* CSMA.

acces multiplu prin divizarea spectrului de frecvențe *vezi* FDMA.

acces multiplu prin divizarea timpului *vezi* TDMA.

acces protejat Wi-Fi *vezi* WPA.

adresă IP Adresă numerică care corespunde unei conexiuni dintre un dispozitiv de rețea și o rețea. De exemplu, fiecare placă de rețea fără fir va avea o adresă IP. Fiecare placă de rețea trebuie să aibă asociată o adresă IP dacă utilizatorul vrea să folosească aplicații TCP/IP, cum ar fi transmiterea și primirea de e-mail-uri, navigarea pe Web sau conectarea la un server de aplicație de corporație.

antena Dispozitiv fizic care convertește semnalele electrice în unde radio sau în unde de lumină — și viceversa — pentru propagarea prin mediul aerian. Antenele pot fi omnidirecționale, care emit undele radio în toate direcțiile, sau direcționale, care concentrează undele radio mai ales pe o anumită direcție.

antena direcțională Tip de antena care concentrează undele radio emise într-o direcție preferențială. Antenele direcționale fac parte, în mod obișnuit, din sistemele MAN fără fir și din cele WAN fără fir. Antenele direcționale au o distanță de acțiune mai mare pe o direcție și mai mică în toate celelalte direcții.



asociere Proces prin care o stație 802.11 (dispozitiv de calcul) devine o parte a unei LAN fără fir. După asociere, utilizatorul poate folosi serviciile oferite de rețea.

autentificare Proces de dovedire a identității unui utilizator sau a unei stații de bază. Utilizarea numelui de utilizator și a parolei este o metodă comună de autentificare, dar există multe alte mecanisme de autentificare mai sofisticate. De exemplu, certificatele digitale pot oferi mijloacele necesare pentru o autentificare realizată fără intervenția utilizatorului.

Bluetooth Specificație publicată de Bluetooth Special Interest Group care definește caracteristicile radio și funcționarea unei rețele de radio frecvență de mică putere și de rază de acțiune scurtă. Astăzi, multe dispozitive au implementat specificația Bluetooth, însă grupul 802.15 dezvoltă standardele corespunzătoare.

CDMA (code division multiple access) Proces în care fiecare utilizator modulează semnalul folosind un cod diferit, care nu generează interferențe.

CDPD (Cellular Digital Packet Data) Tehnică care permite transmiterea datelor printr-un sistem de telefonie celulară analogică, cu viteze de transmisie de 19,2 Kbps. CDPD începe să fie considerat învechit, pe măsură ce devin disponibile noile sisteme 3G.

certificat digital Mesaj electronic care conține acreditările unui anumit utilizator. Certificatele digitale sunt utilizate ca un mijloc de autentificare a utilizatorilor sau a dispozitivelor lor de calcul.

CF (CompactFlash) Placă de rețea de mici dimensiuni folosită la PDA-uri, camere video și alte dispozitive de calcul de mici dimensiuni. Plăcile CF pentru sisteme Bluetooth și 802.11 sunt disponibile pe scară largă.

criptare Modificarea biților de date în concordanță cu o cheie, înainte de transmiterea acestora prin rețea. WEP și WPA sunt exemple de criptări folosite în LAN-urile fără fir.

criptare WEP *vezi* WEP.

CSMA (carrier sense multiple access) Proces care permite ca mai multe stații 802.11 să partajeze mediul aerian comun. Stațiile încearcă să transmită date doar atunci când nici o altă stație nu transmite. În caz contrar apar coliziuni, iar stația respectivă trebuie să retransmită datele.

curios (snooper) Persoană care produce accidental — de obicei din neglijență — întreruperea funcționării unei rețele fără fir.

date Informații, cum sunt fișierele electronice, care sunt stocate și transmise printr-o rețea fără fir. Adesea, datele sunt transmise în mai multe pachete, care sunt transportate separat prin rețea.

DCF (distributed coordination function) Parte a standardului 802.11 ce definește modul în care stațiile vor concura pentru accesul la mediul aerian. DCF face apel la CSMA pentru a regla traficul din rețea.

DHCP (Dynamic Host Configuration Protocol) Protocol care atribuie dispozitivelor de calcul, în mod automat, adrese IP unice dintr-o plajă stabilită. Majoritatea LAN-urilor fără fir, de locuință sau publice, implementează DHCP, ceea ce ușurează obținerea accesului la rețea de către utilizatori. DHCP atribuie automat adrese IP valide acestor utilizatori.

dispozitiv client Hardware care are o interfață cu utilizatorul ce permite folosirea aplicațiilor rețelelor fără fir. Dispozitiv client este un alt nume pentru dispozitiv de calcul.

dispozitiv de calcul Orice punct final al unei rețele fără fir, cum ar fi un laptop, un PDA sau un robot. Este numit adesea și dispozitiv client.

DSSS (direct sequence spread spectrum) Tip de spectru larg în care un cod de împrăștiere crește viteza de transfer a fluxului de date prin difuzarea semnalului pe o porțiune mai largă a spectrului de frecvențe. LAN-urile fără fir 802.11b folosesc DSSS.

emularea terminalului Mecanism prin care utilizatorii obțin o interfață cu o rețea, prin intermediul unor aplicații care rulează pe un calculator central. VT220, 3270 și 5250 sunt tipuri de emulare a terminalului.

Ethernet Denumire dată LAN-urilor cu fir conforme standardului 802.3. Ethernet este un tip de rețea comun, utilizat de companii pentru interconectarea PC-urilor și serverelor. Rețelele Ethernet realizează sistemul de distribuție pentru majoritatea LAN-urilor fără fir.

FDMA (frequency division multiple access) Proces care împarte o bandă de frecvență relativ largă în sub-benzi de lărgimi mai mici, fiecare utilizator transmițând vocea și datele pe sub-banda care i-a fost atribuită.

FHSS (frequency hopping spread spectrum) Tip de spectru larg în care transceiverele fac salturi de la o frecvență la alta, în concordanță cu un model cunoscut de salturi, pentru a împrăști semnalul pe o porțiune mai largă a benzii de frecvență. LAN-urile fără fir 802.11b mai vechi utilizează FHSS.

fibră optică Bucată lungă de sticlă, de diametru mic, îmbrăcată într-o protecție, care poartă semnalele luminoase. Un cablu cu fibră optică are o îmbrăcăminte protectoare, ceea ce îl face greu de distins de un cablu bazat pe fire din cupru.

frecvență Reprezintă de câte ori pe secundă se produce repetarea semnalului. De regulă este măsurată în Hertzi (Hz), adică în numărul de cicluri dintr-o secundă. De exemplu, frecvențele de funcționare ale LAN-urilor fără fir se află în benzile de 2,4 GHz și de 5 GHz.

FSK (frequency shift-keying) Proces de modulare care produce mici modificări ale frecvenței semnalului purtător pentru a reprezenta informația într-un mod care este potrivit pentru propagarea prin aer.

funcție de coordonare distribuită *vezi DCF.*

furnizor de servicii Internet fără fir *vezi WISP.*

GPS (global positioning system) Sistem care permite unei persoane care deține un dispozitiv GPS să determine cu ușurință poziția sa geografică. GPS oferă baza pentru un sistem de navigație excelent, ca și pentru servicii bazate pe localizare oferite de rețelele fără fir.

hacker Persoană care are dorința și capacitatea de a fura informații aflate într-o rețea. Deseori, hackerii încearcă să pătrundă în sistemele de corporație pentru a se distra și pentru a exploata vulnerabilitățile rețelelor fără fir.

interferență Semnale nedorite care întrerup funcționarea unei rețele fără fir. Prezența interferențelor duce la scăderea performanțelor rețelelor fără fir.

interoperabilitate Capacitatea dispozitivelor de calcul de a realiza cu succes o interfață cu o rețea fără fir.

IP (Internet Protocol) Protocol de direcționare a pachetelor între dispozitivele de calcul atașate la o rețea. IP plasează un antet în fața fiecărui pachet de date, antet care conține adresa IP sursă și adresa IP de destinație ale pachetului respectiv.

IPSec (IP Security) Protocol care oferă suportul pentru protecția schimbului de pachete de date la nivelul stratului rețea al unei rețele. IPSec este implementat, în mod uzual, în VPN-uri și criptează pachetele de date de pe tot cuprinsul rețelei; adesea se face referire la acest lucru ca fiind criptare capăt-la-capăt.

IrDA (Infrared Data Association) Standard pentru aplicații de comunicații seriale de date, interoperabile, pe distanțe scurte, cu costuri și consumuri scăzute, bazate pe semnale de lumină infraroșie. Multe laptopuri și PDA-uri au implementat IrDA.

LAN fără fir Rețea care satisface necesitățile de conectare fără fir pe suprafața unei clădiri sau a unui campus universitar. 802.11 și Wi-Fi sunt standarde populare care definesc LAN-urile fără fir.

LAN fără fir publică Tip de LAN fără fir, cunoscută și sub numele de punct fierbinte, care poate fi accesată de orice persoană care are un dispozitiv de calcul configurat corespunzător.

LDAP (Lightweight Directory Access Protocol) Protocol care asigură accesul la directoare cu informații.

MAN fără fir Rețea care satisface necesitățile de conectare fără fir pe suprafața unui oraș. MAN-urile fără fir utilizează standardul 802.16 și alte standarde brevetate.

mediu Spațiul prin care se propagă semnalele de comunicații (cum ar fi, de exemplu, undele radio). În cazul rețelelor fără fir, mediul este aerul.

mod ad-hoc Configurație a unei rețele fără fir care permite comunicații directe de la un dispozitiv de utilizator la un altul, fără să fie necesar ca traficul să treacă printr-o stație de bază. Modul ad-hoc poate fi aplicat atât în PAN-uri fără fir, cât și în LAN-uri fără fir.

modulare Prin modulare este creat un semnal radio sau un semnal luminos, pornind de la datele rețelei, semnal care este potrivit pentru propagarea prin mediul aerian. Exemple de tipuri de modulare sunt: FSK (modularea în frecvență), PSK (modularea în fază) și QAM (modularea în fază și amplitudine).

modulare în fază *vezi PSK.*

modulare în fază și amplitudine *vezi QAM.*

modulare în frecvență *vezi FSK.*

multiplexare prin divizarea ortogonală a frecvenței *vezi OFDM.*

NAT (Network Address Translation) Protocol care stabilește conexiunile logice dintre adresele IP oficiale și adresele private care pot fi folosite în rețele interne. De exemplu, un furnizor al unui serviciu Internet de bandă largă poate oferi doar o singură adresă IP oficială proprietarului unei locuințe. NAT, împreună cu DHCP, permit proprietarului locuinței să aibă mai multe PC-uri și laptopuri care să partajeze unica adresă IP oficială.

NIC (Network Interface Card) Dispozitiv hardware care realizează interfața cu rețeaua pentru un dispozitiv de calcul. Cunoscută și sub numele placă radio (pentru rețelele fără fir) sau placă client.

NIC radio Tip de placă de rețea (NIC) care transmite și recepționează semnale RF.

OFDM (orthogonal frequency division multiplexing) Proces care împarte un semnal modulat pe mai multe sub-purtătoare, înainte de transmisia prin mediul aerian, pentru a îmbunătăți performanțele. LAN-urile fără fir 802.11a și 802.11g, ca și unele soluții MAN fără fir brevetate, utilizează OFDM.

PAN fără fir Rețea care satisface necesitățile de conectare fără fir dintr-o încăpere mică sau din raza de acțiune a unei persoane. Bluetooth și 802.15 sunt tehnici populare utilizate pentru PAN-urile fără fir.

parafoc Dispozitiv care îi oprește pe utilizatorii conectați la o anumită parte a unei rețele să acceseze resurse importante. Datorită vulnerabilității acestora, punctele de acces ale LAN-urilor fără fir sunt deseori plasate în exteriorul parafocului.

PC card *vezi placă PC.*

PDA (personal digital assistant) Dispozitiv de dimensiuni reduse utilizat de o persoană pentru stocarea de informații de contact, programări și liste de activități/sarcini. Unele PDA-uri rulează programe software, cum ar fi clienți de e-mail sau browsere Web.

placă de rețea *vezi NIC.*

placă PC Dispozitiv de dimensiunile unei cărți de credit care oferă memorie extinsă, modemuri, conectivitate pentru dispozitive externe precum și posibilitate de conectare la rețele fără fir pentru dispozitive de calcul de mici dimensiuni, cum sunt laptopurile și PDA-urile. Multe plăci PC implementează tehnici 802.11 sau Bluetooth.

protocol pentru configurarea dinamică a gazdelor *vezi DHCP.*

protocol pentru traducerea adreselor de rețea *vezi NAT.*

PSK (phase shift keying) Proces de modulare care produce mici modificări ale fazei semnalului purtător pentru a reprezenta informațiile într-un mod potrivit pentru propagarea prin aer.

punct de acces Tip de stație de bază pe care LAN-uri fără fir îl folosesc pentru a realiza interfața între utilizatorii fără fir și rețeaua cu fir și pentru a oferi roaming (adică posibilitatea de conectare pentru dispozitivele de utilizator mobile) în interiorul unei clădiri sau al unui campus.

punct de acces pirat Punct de acces care nu este autorizat și are setări de configurație care pot permite cuiva să obțină accesul la resursele rețelei.

punct fierbinte Locația unei LAN fără fir publice. Punctele fierbinți se află în zone în care se aglomerează persoane care dețin dispozitive de calcul, cum este cazul aeroporturilor, hotelurilor, centrelor de conferințe și cafenelelor.

punte Dispozitiv care interconectează două rețele la nivelul stratului 2 (legătură de date). Puntea retransmite pachetele de date către o altă rețea pe baza adresei MAC găsită în antetul pachetului. Puntea joacă un rol cheie în rețelele MAN fără fir.

QAM (quadrature amplitude modulation) Proces de modulare care produce mici modificări de amplitudine și de fază ale semnalului purtător pentru a reprezenta informațiile într-un mod potrivit pentru propagarea prin aer.

RADIUS (Remote Authentication Dial-In User Service) Sistem de autentificare și evidență pe care îl folosesc mulți furnizori de servicii Internet fără fir (WISP) pentru a realiza controlul accesului și înregistrarea/taxarea în rețelele fără fir.

repetor Dispozitiv care recepționează și retransmite semnalele cu unicul scop de a extinde raza de acțiune a rețelei.

rețea privată virtuală *vezi VPN.*

router Tip de stație de bază care implementează protocoale de rețea speciale, cum sunt DHCP și NAT, care permit utilizatorilor să folosească aplicațiile TCP/IP.

satelit Repetor de semnal localizat pe o orbită în jurul Pământului. Sateliții oferă acoperire WAN fără fir utilizând semnalele radio.

semnal analogic Semnal a cărui amplitudine variază continuu în timp. O undă radio este un exemplu de semnal analogic.

semnal digital Semnal a cărui amplitudine variază în trepte, în funcție de timp. Semnalul digital reprezintă datele în interiorul dispozitivelor de calcul. Semnalul digital trebuie convertit într-o formă analogică — proces numit modulare — înainte ca datele să poată fi transmise prin mediul aerian.

semnal purtător Semnal RF primar care transportă datele prin mediul aerian. Diversele tipuri de modulări modifică frecvența, faza sau amplitudinea semnalului purtător pentru a reprezenta informațiile.

semnal RF Semnal de radiofrecvență destinat propagării prin mediul aerian.

servicii bazate pe localizare Capacitatea de a localiza utilizatorii și de a le livra informații referitoare la poziționarea pe o anumită zonă.

sistem 1G Sistemul de telefonie celulară inițial (prima generație) care utilizează semnale analogice. Acest sistem nu poate asigura, în mod eficient, transmisia datelor din calculatoare.

sistem 2G Primul sistem de telefonie celulară care utilizează semnale digitale (a doua generație) și care asigură viteze de transmisie a datelor sub 20 Kbps.

sistem 3G Versiune modificată a sistemelor 2G (a treia generație) care oferă un suport mai bun pentru comunicațiile de date, cum ar fi viteze de transmisie a datelor mai mari.

sistem de distribuție Sistem cu fir care interconectează fizic punctele de acces dintr-o LAN fără fir. O rețea Ethernet este un sistem de distribuție uzual pentru LAN-urile fără fir.

sistem punct-la-multe-puncte Sistem în care comunicațiile sunt realizate direct de la un utilizator la mai mulți alți utilizatori.

sistem punct-la-punct Sistem în care comunicațiile sunt realizate direct de la un utilizator la un altul.

spectru larg Distribuția semnalului purtător pe o porțiune mai largă a spectrului de frecvențe. Secvența directă (DSSS) și saltul de frecvență (FHSS) sunt două tipuri de spectru larg.

stație de bază Hardware care asigură conectarea fără fir a dispozitivelor de calcul, între ele, precum și la o rețea cu fir. Punctele de acces și routerele fără fir sunt tipuri de stații de bază pentru LAN-uri fără fir.

stratul de control al accesului la mediu (MAC) Parte a arhitecturii de rețea care administrează și întreține comunicațiile printr-un mediu partajat. Stratul MAC este „creierul” unui plăci de rețea sau al unui punct de acces și impune regulile pe care trebuie să le respecte toate dispozitivele din rețea.

TCP (Transmission Control Protocol) Protocol care stabilește și întreține conexiunile dintre dispozitivele de calcul atașate la o rețea. TCP este utilizat împreună cu IP, această combinație fiind numită TCP/IP.

TDMA (time division multiple access) Proces care permite doar unui singur utilizator să transmită într-o fereastră de timp dată. Fiecare utilizator folosește întreaga lărgime de bandă pe perioada ferestrei de timp care îi este atribuită.

transceiver Dispozitiv care transmite și recepționează informații. Transceiverul este localizat pe o placă NIC radio.

viteza de transmisie (a datelor) Numărul de biți de date transmiși într-o secundă. De exemplu, LAN-urile fără fir 802.11b operează la viteze de până la 11 Mbps.

VPN (virtual private network) Utilizarea unui software special, aflat pe un dispozitiv client, care controlează accesul pentru aplicații aflate la distanță și care protejează conexiunea, de la un capăt la celălalt, prin utilizarea criptării.

WAN fără fir Rețea care satisface necesitățile de conectare fără fir pe suprafețe geografice mari, cum ar fi o țară sau un continent. Sateliții oferă mijloacele necesare pentru extinderea transmisiilor de semnale radio prin WAN-urile fără fir.

WEP (Wired Equivalent Privacy) Parte a standardului 802.11 care definește criptarea folosită de dispozitivele conectate la o rețea LAN fără fir.

Wi-Fi Nume de brand dat LAN-urilor fără fir care se conformează standardelor definite și publicate de Wi-Fi Alliance. Standardele Wi-Fi au la bază standardul 802.11.

WISP (wireless Internet service provider) Companie care oferă servicii de conectare fără fir la Internet, pentru locuințe și sedii de firme. Adesea, WISP-urile oferă acces fără fir și la LAN-urile fără fir publice din punctele fierbinți.

WPA (Wi-Fi Protected Access) Protocol de securitate, definit de Wi-Fi Alliance, care permite dispozitivelor de calcul să obțină periodic o cheie nouă pentru criptare. Versiunea 1 a protocolului WPA implementează Temporal Key Integrity Protocol (TKIP) și criptarea WEP, în timp ce versiunea 2 a protocolului WPA implementează în întregime standardul 802.11i (care include AES).

zgomot de fond Amplitudinea semnalelor electromagnetice dintr-o anumită zonă, atunci când rețeaua fără fir nu funcționează.

INDEX

A

acces cu sesizarea purtătoarei, atacuri negare de serviciu (DoS), 176

acces la mediu, 59

CSMA/CA (carrier sense multiple access with collision avoidance), protocol, 118

DCF (distributed coordination function), 118

LAN-uri fără fir, 118–124

acces multiplu prin divizarea spațială (SDMA), 167

acces multiplu prin divizarea spectrului de frecvențe (FDMA), 165

acces multiplu prin divizarea timpului (TDMA), 147, 166

acces neautorizat, amenințări la adresa securității, 171–174

acces protejat Wi-Fi (WPA), 130

activități de teren, aplicații ale

WAN-urilor fără fir în, 20–21

adaptoare USB, PAN-uri fără fir, 90–91

administrarea lărgimii de bandă, controlere de acces, 42

a doua generație de sisteme celulare (sisteme 2G), WAN-uri fără fir, 158

afișarea informațiilor, 58

AirMagnet, 172

AiroPeek, 172

alerte (SMS), 160

amenințări (la adresa securității), 171

accesul neautorizat, 171–174

atacuri de tipul omul-la-mijloc, 174–176

curioși, 172

DoS (denial of service), 171, 176–178

hackeri, 171

monitorizarea pasivă, 171

monitorizarea traficului, 172

amenințări (la adresa securității) de tip DoS (denial of service), 171, 176–178

amplificare, transceivere fără fir, 69

antene

antene direcționale, MAN-uri fără fir, 140–142

LAN-uri fără fir, 110

polarizare, 142

transceivere fără fir, 69

WAN-uri fără fir, 155–156

antene de mare directivitate, MAN-uri fără fir, 141–142

antene direcționale, 140–142

polarizare, 142

antene semidirecționale, MAN-uri fără fir, 141

antete ale pachetelor IP (Internet Protocol), routere, 108

aplicații, aplicații fără fir, 14–21

arhitecturi de rețele, 52–54

asistarea sistemelor finale, middleware, 45

asistența la birou, sisteme de management, 49



asociere la LAN-uri fără fir, 122

atacuri

atacuri de tipul omul-la-mijloc,

174–176

atacuri negare de serviciu (DoS),

176–178

atacuri de tipul omul-la-mijloc,

174–176

atenuare, semnale luminoase, 79

a treia generație de sisteme celulare

(sisteme 3G), WAN-uri fără fir,

159–161

autentificare, 171, 185

autentificare IEEE 802.11, punctele

vulnerabile, 185–186

autentificare IEEE 802.1x, 188–190

certIFICATE digitale, 41

controlere de acces, 42

criptare cu cheie publică, 187–188

filtre MAC, 187

LAN-uri fără fir, 121–122

RADIUS (Remote Authentication

Dial-In User Service), 42

B

benzi de frecvență, LAN-uri fără fir,

alegerea, 128

Bluetooth

LAN-uri fără fir, 97

PAN-uri fără fir, 96–98

interferență, 98–101

specificații, 7

Bluetooth Special Interest Group

(SIG), 96

C

cabinete medicale, LAN-uri fără fir, 113

caracteristici ale semnalelor RF, 70–72

carduri CF (Compact Flash), 36

CDMA (code division multiple

access), 166

CDPD (Cellular Digital Packet Data), 13

certIFICATE digitale, 41

comasarea de date, middleware, 45

companii care vând prin automate,

WAN-uri fără fir, aplicații ale, 21

companii furnizoare de utilități,

WAN-uri fără fir, aplicații ale, 20

comunicații bazate pe arderea meteo-

rilor, WAN-uri fără fir, 164

conectivitate directă de

baze de date, 44

conexiuni, 65–66

punți, MAN-uri fără fir, 138–140

conexiuni la Internet, PAN-uri fără

fir, sisteme pentru locuințe și firme

mici, 94

configurare

configurații de bază, 14

dispozitive fără fir, verificarea,

192–193

management, sisteme de

management, 49

puncte de acces, 107

stații de bază, monitorizarea, 198

controlere de acces, 40–42

administrarea lărgimii de bandă, 42

autentificare, 42

avantajele, 41

criptare, 42

roaming-ul de subrețea, 42

criptare, 171, 178–180

controlere de acces, 42

criptare cu cheie publică, 179–180,

187–188

criptare simetrică, 179

politici, 195

VPN-uri (virtual private networks),

185

WEP (Wired Equivalent Privacy),

178, 181–183

TKIP (Temporal Key Integrity

Protocol), 183–184

WPA (Wi-Fi Protected Access), 184

criptare cu cheie publică, 179–180,

187–188

criptare simetrică, 179

criptare WEP. *Vezi* WEP

CSMA/CA (carrier sense multiple

access with collision avoidance),

protocol, 118

curioși (snoopers), 172

D

DCF (distributed coordination

function), 118

desfășurarea de controale, 198

DHCP (Dynamic Host Configuration

Protocol), 108

discuții cu utilizatorii, 192

dispozitive de calcul, 32

infrastructuri, 38–48

mediul aerian, 37–38

rețele fără fir, 31, 33–34

NIC-uri (*network interface cards*),

34–37

sisteme de management, 48–51

dispozitive fără fir, configurații,

verificarea, 192–193

dispozitive pentru utilizator

LAN-uri fără fir, 105

PAN-uri fără fir, 89–90

WAN-uri fără fir, 152

acceptarea mai multor tehnici, 167

antene, 155–156

NIC-uri radio, 153–154

stații de bază, 154–155

distorsionare

semnale luminoase, 78

atenuare, 79

interferențe, 79

semnale RF

interferențe, 73–74

propagare pe mai multe căi, 74–76

DMZ-uri (demilitarized zones) fără

fir, 195

domeniul îngrijirii sănătății, LAN-uri

fără fir, aplicații în, 17

DSSS (direct sequence spread

spectrum), strat fizic, 124

E

emițătoare, transceivere fără fir, 69

emularea terminalului, 43

Ethernet, 106

examinări RF ale locațiilor, LAN fără fir de întreprindere, 113

F

factori de formă, NIC-uri (network interface cards), 35–37

carduri CF (CompactFlash), 36

ISA (Industry Standard Architecture), 35

PCI (Peripheral Component Interconnect), 35

plăci mini-PCI, 35

plăci PC, 35

factori de formă CF (CompactFlash), PAN-uri fără fir, 90

FDMA (frequency division multiple access), 165

FHSS (frequency hopping spread spectrum), strat fizic, 124

filtre MAC, 187

filtre MAC, autentificare, 187

flux continuu de multimedia, PAN-uri fără fir, sisteme pentru locuințe și firme mici, 92–93

flux de informații, rețele fără fir, 57
conexiuni, 65–66
mediu aerian, 59–64
puncte finale, 57–58
transferul semnalului purtător de date, 65

fragmentare, LAN-uri fără fir, 123

frecvențe, semnale RF, 72

FSK (frequency shift-keying), 81

funcția de coordonare distribuită (DCF), 118

H

hackeri, 171

Hertz, 57

HiperLAN/2 (High Performance Radio LAN), LAN-uri fără fir, 131–133

hoteluri, LAN-uri fără fir, 116

I

identificatorul setului de servicii (SSID), puncte de acces, 107
imobiliar, rețele fără fir, aplicații pentru domeniul, 19

Industry-Standard Architecture (ISA), 35

Infrared Data Association (IrDA). *Vezi*

IrDA (Infrared Data Association)
infrastructura, rețele fără fir, 31

infrastructuri, 38–48

controlere de acces, 40–42

sisteme de distribuție, 46–48

software pentru conectivitatea aplicațiilor, 42–45

stații de bază, 38–42

instituții de învățământ, LAN-uri fără fir, aplicații pentru, 18

integrarea în aplicații (SMS), 160

interactivitate (SMS), 160

interferență

Bluetooth, minimizarea, 98–101

semnale luminoase, 79

semnale RF, 73–74

interoperabilitate, NIC-uri radio, LAN-uri fără fir, 106

introducerea informațiilor, 58

IPSec, 42

IrDA (Infrared Data Association), PAN-uri fără fir, 101–102

ISA (Industry-Standard Architecture), NIC-uri, 35

Î

întreținere, sisteme de management, 51

L

LAN-uri Ethernet, compartie cu

LAN-urile fără fir, 8

LAN-uri fără fir, 5, 7–8, 105

antene, 110

aplicații, 14–21

instituții de învățământ, 18

îngrijirea sănătății, 17

verificarea inventarelor, 17

avantaje ale, 24–27

benzi de frecvență, alegerea, 128

Bluetooth, 97

dispozitive pentru utilizatori, 105

HiperLAN/2 (High Performance Radio LAN), 131–133

hoteluri, 116

LAN-uri de întreprindere, 112–114

LAN-uri Ethernet, comparație cu, 8

LAN-uri fără fir ad-hoc, 117

LAN-uri fără fir publice, 114–116

LAN-uri pentru locuințe și firme mici, 111–112

NIC-uri radio, 106

puncte de acces, 106–107

repetoare, 109–110

routeri, 108–109

spitale, 113

standardul IEEE 802.11, 9, 118–120
asociere, 122

autentificare, 121–122

fragmentare, 123

modul economie de energie, 123

RTS/CTS, 122

scanare, 120

straturi fizice, 124–129

stratul MAC, 118–124

WEP, 122

tipuri de rețele fără fir, comparație cu, 13–14

Wi-Fi (Wireless Fidelity), 9, 130–131

LAN-uri fără fir ad-hoc, 117

LAN-uri fără fir de întreprindere, 112–114

LAN-uri fără fir publice, 114–116

lărgime de bandă, 55

LDAP (Lightweight Directory Access Protocol), 42

legătura cu mediul aerian, 59–64

legături simplex, 64

Lightweight Directory Access Protocol (LDAP), 42

linii duplex complet, 64

linii semiduplex, 64

livrări de conținut (SMS), 160

M

MAN-uri fără fir, 5, 9–11

antene direcționale, 140–142

aplicații, 14–21

avantaje ale, 24–27, 137

punți, 138–140

puncte de acces, 139

punți Ethernet-la-rețea-fără-fir, 139

punți grup de lucru, 140

sisteme punct-la-multe-puncte,
143–144

sisteme punct-la-punct, 142–143

sisteme radio cu pachete, 144–145

standardul 802.11, 145

standardul 802.16, 146–147

tehnici, 145

tipuri de rețele fără fir, comparație cu,
13–14

Wi-Fi, 145

WISP-uri (Wireless Internet Service
Providers), 10

mediu aerian, 37–38

realizarea interfeței cu, 59–64

semnale, 31

middleware (fără fir), 44–45

**modelul de referință OSI (Open
Systems Interconnect), 52**

**modificarea configurație ecranelor,
middleware, 45**

modulare

emițătoare ale transceiverelor fără fir,
69

propagarea semnalelor, pregătirea
pentru, 80–86

modulare în fază (PSK), 82

**modulare în fază și amplitudine
(QAM), 82–83**

modulare în frecvență (FSK), 81

**modul economie de energie, LAN-uri
fără fir, 123**

**monitorizarea pasivă, amenințări la
adresa securității, 171**

**monitorizarea rețelei, sisteme de
management, 50**

**monitorizarea traficului, amenințări
la adresa securității, 172**

**multiplexare, OFDM (Orthogonal
Frequency Division
Multiplexing), 146**

N

**negare de serviciu (DoS), amenințări,
171, 176–178**

**NIC-uri (network interface cards),
34–37**

factori de formă, 35, 37

carduri CF (CompactFlash), 36

*ISA (Industry-Standard
Architecture), 35*

*PCI (Peripheral Component
Interconnect), 35*

plăci Mini-PCI, 35

plăci PC, 35

NIC-uri radio, LAN-uri fără fir, 106

NIC-uri radio

LAN-uri fără fir, 106

PAN-uri fără fir, 90

WAN-uri fără fir, 153–154

noduri, transmisii de date, 60

O

obstacole, semnale luminoase, 79

**OFDM (Orthogonal Frequency
Division Multiplexing), 85, 146**

P

PAN-uri fără fir, 5–7, 89

adaptoare USB, 90–91

aplicații, 14–21

avantaje ale, 24–27

Bluetooth, 96–98

interferență, 98–101

specificații, 7

dispozitive pentru utilizator, 89–90

IrDA (Infrared Data Association),
101–102

NIC-uri radio, 90

router, 91

sisteme de întreținere, 94

sisteme pentru locuințe și firme mici, 92

conexiuni la Internet, 94

flux continuu de multimedia, 92–93

legătura cu perifericele, 93

sincronizare, 92

tipărire, 93–94

standardul IEEE 802.15, 7, 95

tipuri de rețele fără fir, comparație cu,
13–14

transceivere, 6

unde radio, 7

viteze de transmisie a datelor, 5

parafooci, 173

actualizare, 196

parafooci personale, implementarea,
198

utilizatori, plasarea în exteriorul, 195

parafooci personale,

implementarea, 198

parole, stații de bază, atribuirea de, 197

**PCMCIA (Personal Computer
Memory Card International
Association), plăci PC, 35**

**plăci de rețea (NIC-uri). Vezi NIC-uri
(network interface cards)**

plăci mini-PCI, 35

plăci PC, 35

**plăci PCI (Peripheral Component
Interconnect), 35**

polarizare, antene, 142

politici (de securitate), 190–191

criptare, 195

desfășurarea de controale, 198

dispozitive fără fir, verificări de
configurație, 192–193

DMZ-uri (demilitarized zones) fără
fir, 195

evaluări, 191–194

îmbunătățiri, recomandarea de, 194

lacune de securitate, analizarea, 194

parafooci, 195

actualizare, 196

parafooci personale,

implementarea, 198

propagarea undelor radio,

limitarea, 197

revizuirea sistemelor, 192

revizui, 191

SSID-uri, 197

stații de bază, 196–197

monitorizarea configurațiilor, 198

stabilirea parolelor, 197



stații de bază pirat, identificarea, 193
 teste de penetrare, 194
 utilizatori, discutarea cu, 192
porți, 39
porți de rezidență, 39
prima generație de sisteme celulare (sisteme 1G), 158
proces de spectru larg, modular, 83–85
propagarea, unde radio, limitarea, 197
propagarea pe mai multe căi, 65
 semnale RF, 74–76
protocoale, 41
protocol de integritate cu cheie temporară (TKIP), 183–184
protocol pentru configurarea dinamică a gazdelor (DHCP), 108
protocol pentru controlul transmisiei (TCP), 53
protocolul NAT (Network Address Translation), 108
PSK (phase shift-keying), 82
puncte de acces, 38
 asociere la LAN-uri fără fir, 122
 configurare, 107
 LAN-uri fără fir, în 106–107
 puncte de acces pirat, 173
 punți, comparație cu, 139
 SSID (service set identifier), 107
puncte de acces pirat, 173
puncte de acces pirat, identificarea, 193
puncte fierbinți, LAN-uri fără fir publice, 114

puncte finale, flux de informații, 57–58
punți
 puncte de acces, comparație cu, 139
 MAN-uri fără fir, 138–140
 punți Ethernet-la-rețea-fără-fir, 139
 punți grup de lucru, 140
punți Ethernet-la-rețea-fără-fir, 139
punți grup de lucru, 140

Q

QAM (quadrature amplitude modulation), 82–83

R

RADIUS (Remote Authentication Dial-In User Service), 42
raportarea, sisteme de management, 50
receptoare
 emițătoare, 69
 transceivere fără fir, 69
Remote Authentication Dial-In User Service (RADIUS), 42
repetoare, LAN-uri fără fir, 109–110
reporniri inteligente, middleware, 45
reproiectare, sisteme de management, 51
rețele extinse (WAN-uri). Vezi WAN-uri fără fir
rețele fără fir, 3–10
 avantaje ale, 24–27
 dispozitive de calcul, 31–34
 infrastructuri, 38–48
 medii aeriene, 37–38
 sisteme de management, 48–51

fluxul de informații, 57
 conexiuni, 65–66
 mediul aerian, 59–64
 puncte finale, 57–58
 transferul semnalelor purtătoare de date, 65
 NIC-uri pentru dispozitive de calcul, 34–37
 stații de bază, 31
 tipuri, comparație, 13–14
 utilizatori, 32
rețele locale (LAN-uri). Vezi LAN-uri fără fir
rețele metropolitane (MAN-uri). Vezi MAN-uri fără fir
rețele personale (PAN-uri). Vezi PAN-uri fără fir
rețele private virtuale (VPN-uri), 185
rețele publice, rețele fără fir, aplicații ale, 21
roaming de subrețea, controlere de acces, 42
router, 39
 antete ale pachetelor IP, 108
 LAN-uri fără fir, 108–109
 PAN-uri fără fir, 91
 tabele de direcționare, 108
router de rezidență, 39
RTS/CTS, LAN-uri fără fir, 122

S

salturi de frecvență în spectru larg (FHSS), stratul fizic, 124
SanDisk Corporation, carduri CF (CompactFlash), 36

sateliți

stații de bază, WAN-uri fără fir, 154–155
 WAN-uri fără fir, 161–163
scanarea LAN-urilor fără fir, 120
SDMA (spatial division multiple access), 167

securitate

amenințări la adresa securității, 171
 accesul neautorizat, 171–174
 atacuri de tipul omul-la-mijloc, 174–176
 curioși, 172
 hackeri, 171
 monitorizarea pasivă, 171
 monitorizarea traficului, 172
 negarea de serviciu (DoS), 171, 176–178
 autentificare, 171, 185
 certificate digitale, 41
 controlere de acces, 42
 criptare cu cheie publică, 187–188
 filtre MAC, 187
 IEEE 802.1x, 188–190
 punctele vulnerabile ale autentificării IEEE 802.11, 185–186
 criptare, 171, 178–180
 acces, 42
 criptare cu cheie publică, 179–180
 criptare simetrică, 179
 VPN-uri (virtual private networks), 185
 WEP (Wired Equivalent Privacy), 178, 181–184

- WPA (Wi-Fi Protected Access), 184
 parafocuri, 173
 politici, 190–191
 analizarea lacunelor de securitate, 194
 criptarea, 195
 desfășurarea de controale, 198
 discuții cu utilizatorii, 192
 DMZ-uri (demilitarized zones) fără fir, 195
 evaluări, 191–194
 identificarea stațiilor de bază pirat, 193
 parafocuri, 195–196
 parafocuri personale, 198
 propagarea undelor radio, 197
 recomandări pentru îmbunătățiri, 194
 revizuirea, 191
 revizuirii ale sistemelor, 192
 SSID-uri, 197
 stații de bază, 196–198
 teste de penetrare, 194
 verificarea configurațiilor dispozitivelor fără fir, 192–193
 roaming de subrețea, controlere de acces, 42
 sisteme de management, 48
secvență directă în spectru larg (DSSS), stratul fizic, 124
semnale
 luminoase (de lumină), 69, 76
 atenuarea, 79
 avantaje, 78
 caracteristici, 76–77
 dezavantaje, 78
 distorsionări, 78
 interferență, 79
 mediul aerian, 31
 mediile aeriene, 37–38
 modulare, 80–83
 FSK (frequency shift-keying), 81
 OFDM (Orthogonal Frequency Divison Multiplexing), 85
 PSK (phase shift-keying), 82
 proces de spectru larg, 83–85
 QAM (quadrature amplitude modulation), 82–83
 UWB (ultrawideband), 86
 propagare
 pregătire pentru, 80–86
 RF (radiofrecvență), 69–70
 avantaje, 72
 caracteristici, 70–72
 dezavantaje, 72
 frecvențe, 72
 interferență, 73–74
 propagare pe mai multe căi, 74–76
 semnale purtătoare, 80
 semnale care transmit informații, 54
 semnale analogice, 56–57
 semnale digitale, 54–56
 transferarea, 65
semnale analogice, 56–57
semnale care transmit informații, 54
 semnale analogice, 56–57
 semnale digitale, 54–56
semnale de radiofrecvență (RF). Vezi semnale RF

- semnale digitale**, 54–56
 transfer, 56
 viteze de transmisie a datelor, 55
semnale luminoase, 69, 76
 avantaje, 78
 caracteristici, 76–77
 dezavantaje, 78
 distorsionări, 78
 atenuare, 79
 interferență, 79
 modulare, 80–83
 FSK (frequency shift-keying), 81
 OFDM (Orthogonal Frequency Divison Multiplexing), 85
 PSK (phase shift-keying), 82
 proces de spectru larg, 83–85
 QAM (quadrature amplitude modulation), 82–83
 UWB (ultrawideband), 86
 propagare, *pregătire pentru*, 80–86
semnale purtătoare, 80
semnale purtătoare de date,
transferul, 65
semnale RF, 69–70
 avantaje, 72
 caracteristici, 70–72
 dezavantaje, 72
 distorsionări, 78
 interferență, 73–74
 propagare pe mai multe căi, 74–76
 frecvențe, 72
 modulare, 80–83
 FSK (frequency shift-keying), 81
 OFDM (Orthogonal Frequency Divison Multiplexing), 85
 PSK (phase shift-keying), 82
 proces de spectru larg, 83–85
 QAM (quadrature amplitude modulation), 82–83
 UWB (ultrawideband), 86
 propagare, *pregătire pentru*, 80–86
PSK (phase shift-keying), 82
proces de spectru larg, 83–85
QAM (quadrature amplitude modulation), 82–83
UWB (ultrawideband), 86
 propagare, *pregătire pentru*, 80–86
servicii bazate pe localizare, WAN-uri fără fir, aplicații, 23
serviciul de mesaje scurte (SMS), 160
sincronizare, PAN-uri fără fir,
sisteme pentru locuințe și firme mici, 92
sisteme de distribuție, 46–48, 106
sisteme de întreprindere, PAN-uri fără fir, 94
sisteme de management, 48–51
 asistența la birou, 49
 întreținere, 51
 managementul configurației, 49
 monitorizarea rețelei, 50
 raportarea, 50
 reproiectarea, 51
 securitatea, 48
sisteme de telefonie, 16
sisteme pentru locuințe și (sedii de) firme mici
 LAN-uri fără fir, 111–112
 PAN-uri fără fir, 92
 conexiuni la Internet, 94
 fluxul continuu de multimedia, 92–93
 legătura cu perifericele, 93
 sincronizare, 92
 tipărire, 93–94

sisteme pentru (sedii de) firme mici

- LAN-uri fără fir, 111–112
- PAN-uri fără fir, 92
 - conexiuni la Internet, 94
 - fluxul continuu de multimedia, 92–93
 - legătura cu perifericele, 93
 - sincronizare, 92
 - tipărire, 93–94
- sisteme punct-la-multe-puncte, MAN-uri fără fir, 143–144
- sisteme punct-la-punct, MAN-uri fără fir, 142–143
- sisteme radio cu pachete, MAN-uri fără fir, 144–145
- SMS (short message service), 160
- software pentru conectivitatea aplicațiilor, 42–45
 - conectivitate directă de baze de date, 44
 - emularea terminalului, 43
 - middleware fără fir, 44–45
- spitale, LAN-uri fără fir, 113
- SSID-uri (service set identifiers)
 - difuzare, dezactivarea, 197
 - puncte de acces, 107
- standardul IEEE 802.11
 - autentificare, 185–186
 - LAN-uri fără fir, 9, 118–120
 - asociere, 122
 - autentificare, 121–122
 - fragmentare, 123
 - modul economie de energie, 123
 - RTS/CTS, 122

- scanare, 120
- straturi fizice, 124–129
- stratul MAC, 118–124
 - WEP, criptarea, 122
- MAN-uri fără fir, 145
- standardul IEEE 802.15, PAN-uri fără fir, 7, 95
- standardul IEEE 802.16, MAN-uri fără fir, 146–147
- standardul 802.1x, autentificare, 188–190
- stații de bază, 31, 38–42
 - configurații, monitorizarea, 198
 - parole, atribuirea, 197
 - porți, 39
 - protejarea fizică, 196–197
 - puncte de acces, 38
 - routeri, 39
 - stații de bază pirat, identificarea, 193
 - WAN-uri fără fir, 154–155
- stocarea informației, 58
- straturi fizice (IEEE 802.11), LAN-uri fără fir, 124–129
- stratul aplicație (stratul 7), modelul de referință OSI, 52
- stratul fizic (stratul 1), modelul de referință OSI, 53
- stratul legătură de date (stratul 2), modelul de referință OSI, 53
- stratul MAC (IEEE 802.11), LAN-uri fără fir, 118–124
- stratul prezentare (stratul 6), modelul de referință OSI, 52
- stratul rețea (stratul 3), modelul de referință OSI, 53

- stratul sesiune (stratul 5), modelul de referință OSI, 53
- stratul transport (stratul 4), modelul de referință OSI, 53

T

- tabele de direcționare, 108
- TCP (Transmission Control Protocol), 53
- TDMA (time division multiple access), 147, 166
- tehnici de optimizare, middleware, 45
- telefoane mobile, acceptarea mai multor tehnici, 167
- teste de penetrare, realizarea de, 194
- tipărire prin intermediul PAN-urilor fără fir, sisteme pentru locuințe și firme mici, 93–94

TKIP (Temporal Key Integrity Protocol), 183–184

transceivere (fără fir), 69–70

- amplificare, 69
- antene, 69
- emițătoare, 69
- PAN-uri fără fir, 6

transferarea, semnale digitale, 56

transmisii, mediul aerian, 31

transmisii de date, mediul aerian, realizare interfeței cu, 59–61

U

- UMTS-uri (Universal Mobile Telecommunications Systems), 159
- unde radio

- PAN-uri fără fir, 7
- propagare, limitarea, 197
- universități, LAN-uri fără fir, aplicații ale, 18
- utilizatori

- discuții cu, 192
- rețele fără fir, 32

V

verificarea inventarelor, LAN-uri fără fir, 17

viteze de transmisie a datelor

- PAN-uri fără fir, 5
- semnale digitale, 55

voce transmisă fără fir, 16

VPN-uri (virtual private networks), 185

W

WAN-uri fără fir, 5, 11–13, 151

- aplicații, 14–21
 - activități de teren, 20
 - companii care vând prin automate, 21
 - companii furnizoare de utilități, 20
 - servicii bazate pe localizare, 23
- avantaje ale, 24–27
- CDMA (code division multiple access), 166
- CDPD (Cellular Digital Packet Data), 13
- dispozitive pentru utilizator, 152
 - acceptarea mai multor tehnici, 167
- antene, 155–156
- NIC-uri radio, 153–154
- stații de bază, 154–155

FDMA (frequency division multiple access), 165

SDMA (spatial division multiple access), 167

TDMA (time division multiple access), 166

tehnici, 165

tipuri de rețele fără fir, comaprație cu, 13-14

WAN-uri fără fir bazate pe spațiu (cosmic), 161

comunicații bazate pe arderea meteorilor, 164

sateliți, 161-163

WAN-uri fără fir pe bază de rețelele celulare, 157-160

a doua generație de sisteme celulare (sisteme 2G), 158

a treia generație de sisteme celulare (sisteme 3G), 159-161

prima generație de sisteme celulare (sisteme 1G), 158

WAN-uri fără fir bazate pe spațiu (cosmic), 161

comunicații bazate pe arderea meteorilor, 164

sateliți, 161-163

WAN-uri fără fir bazate pe rețelele celulare, 157-160

a doua generație de sisteme celulare (sisteme 2G), 158

a treia generație de sisteme celulare (sisteme 3G), 159-161

prima generație de sisteme celulare (sisteme 1G), 158

WEP (Wired Equivalent Privacy), 178, 181-183

LAN-uri fără fir, 122

TKIP (Temporal Key Integrity

Protocol), 183-184

Wi-Fi (Wireless Fidelity)

LAN-uri fără fir, 9, 130-131

MAN-uri fără fir, 145

Wi-Fi Alliance, 130

WISP-uri (wireless Internet service providers), 10, 39

WPA (Wi-Fi Protected Access), 130, 184

Z

zgomot de fond, 61

BIBLIOTECA JUDEȚEANĂ
Panait Istrati BRAILA

Dragi prieteni,

Avem plăcerea să vă invităm la clubul **DEVORATORII DE CARTE IT-CORINT**. COMPLETAȚI acest talon cu numărul exemplarelor dorite și puneți-l netimbrat în orice cutie poștală.

AVANTAJELE DE A FI MEMBRU AL CLUBULUI:

- primiți periodic catalogul aparițiilor editoriale;
- primiți cărțile solicitate, prin poștă, direct la domiciliu, iar taxele poștale sunt suportate de editură;
- primiți câte o carte cadou pentru fiecare nou membru pe care îl aduceți în clubul nostru;
- dacă veți comanda până la 30 de exemplare, beneficiați de o reducere de 10%;
- pentru comenzi mai mari de 30 de exemplare, beneficiați de o reducere de 15%;
- tirajele fiind limitate, acordăm prioritate membrilor clubului **DEVORATORII DE CARTE IT-CORINT**.

Editura își rezervă dreptul de a face modificări de preț, periodic.

La prima comandă făcută de noul membru al clubului **DEVORATORII DE CARTE IT-CORINT** adus de dvs., primiți o carte cadou.

Menționați ce domenii sau lucrări v-ar interesa să regăsiți în aparițiile de la Editura CORINT:

EXPEDITOR: Nume:
Adresa: localitate: str:
nr: bl: sc: ap: cod poștal: jud (sect):.....
☎ telefon:
Numele noului membru al clubului **DEVORATORII DE CARTE IT-CORINT** adus de tine:

NR. EX.	TITLU	AUTORI	PREȚ (lei)
COLECȚIA IT			
	Inițiere în design	Robin Williams	136 000
	Design pentru Web	Robin Williams, John Tollett	326 000
	Dictionar explicativ de calculatoare și Internet	Random House Webster's	153 000
	QuarkXPress 4 și 5. Shortcuts pentru PC și MAC	David Blatner	131 000
	Microsoft Office XP pentru Windows	Steve Sagman	271 000
	Inițiere în Windows XP	Larry Magid	245 000
	Tehnici avansate de design. Adobe Photoshop 7 și Adobe Illustrator 10	Luanne Seymour Cohen	399 000
	Macromedia Dreamweaver MX în 24 de lecții	Betsy Bruce	354 000
	Aventuri în calculator	Sorana Stoica	82 000
	Internet. Ghid complet de utilizare	Linda Bird	375 000
	Photoshop 7 pentru Windows și Macintosh	Elaine Weinmann, Peter Lourekas	382 000
	HTML pentru World Wide Web cu XHTML și CSS	Elizabeth Castro	409 000
	JavaScript pentru World Wide Web	Tom Negrino, Dori Smith	375 000
	QuarkXPress 6 pentru Windows și Macintosh	Elaine Weinmann, Peter Lourekas	399 000
	Visual Basic .NET pentru Windows	Harold Davis	399 000
	Microsoft OFFICE 2003 pentru Windows	Steve Sagman	299 000
	Fotografia digitală: ghid rapid pentru începători	J. Ciaglia, B. London, J. Upton	299 000
	Realizarea filmelor cu Windows XP	Jan Ozer	180 000
	Primii pași în rețele de calculatoare	Wendell Odom	350 000
	Învăț singur PHP, MySQL® și Apache	Julie C. Meloni	500 000
	Primii pași în rețele fără fir	Jim Geier	300 000

Correspondență
Răspuns

CR

Se taxează la
destinație

DESTINATAR:
DEVORATORII DE
CARTE IT-CORINT

CORINT

CP 1 - 591

Cod poștal: 70700

Tel: (021) 222.19.49

București